亚马逊云科技

Service Authorization Reference

Service Authorization Reference

Service Authorization Reference: Service Authorization Reference

Table of Contents

Reference **1**
Actions, resources, and condition keys 1
Actions table 1
Resource types table 2
Condition keys table 3
Amazon Account Management 9
Apache Kafka APIs for Amazon MSK clusters 16
Amazon API Gateway 23
Amazon API Gateway Management 27
Amazon API Gateway Management V2 58
Amazon App Mesh 77
Amazon AppConfig 89
Amazon Application Auto Scaling 106
Amazon Application Recovery Controller - Zonal Shift 114
Amazon AppSync 125
Amazon Athena 142
Amazon Backup 158
Amazon Backup Gateway 178
Amazon Backup storage 185
Amazon Batch 189
Amazon Billing 204
Amazon Billing Console 212
Amazon Budget Service 215
Amazon Certificate Manager 221
Amazon Web Services Cloud Map 228
Amazon CloudAssist service read write permissions 237
Amazon CloudFormation 239
Amazon CloudFront 265
Amazon CloudTrail 292
Amazon CloudWatch 312
Amazon CloudWatch Application Insights 325
Amazon CloudWatch Logs 331
Amazon CloudWatch Observability Access Manager 352
Amazon CloudWatch Synthetics 359

Amazon CodeBuild 367
Amazon CodeCommit 461
Amazon CodeDeploy 481
Amazon CodeDeploy secure host commands service 493
Amazon CodePipeline 495
Amazon Cognito Identity 505
Amazon Compute Optimizer 513
Amazon Config 523
Amazon Connector Service 551
Amazon Consolidated Billing 553
Amazon Cost and Usage Report 555
Amazon Cost Explorer Service 560
Amazon Data Lifecycle Manager 575
Amazon Database Migration Service 579
Amazon Direct Connect 616
Amazon Directory Service 632
Amazon DynamoDB 655
Amazon DynamoDB Accelerator (DAX) 680
Amazon EC2 688
Amazon EC2 Auto Scaling 1569
Amazon EC2 Image Builder 1598
Amazon EC2 Instance Connect 1633
Amazon EKS Auth 1638
Amazon Elastic Beanstalk 1640
Amazon Elastic Block Store 1660
Amazon Elastic Container Registry 1665
Amazon Elastic Container Service 1677
Amazon Elastic File System 1711
Amazon Elastic Kubernetes Service 1722
Amazon Elastic Load Balancing 1742
Amazon Elastic Load Balancing V2 1761
Amazon Elastic MapReduce 1795
Amazon ElastiCache 1814
Amazon Elemental MediaConvert 1878
Amazon EMR Serverless 1888
Amazon EventBridge 1894

Amazon Fapiao Management 1912
Amazon Free Tier 1914
Amazon FreeRTOS 1916
Amazon FSx 1922
Amazon GameLift 1945
Amazon Glue 1973
Amazon Glue DataBrew 2027
Amazon GuardDuty 2036
Amazon Health APIs and Notifications 2052
Amazon IAM Access Analyzer 2057
Amazon IAM Identity Center (successor to Amazon Single Sign-On) 2065
Amazon IAM Identity Center (successor to Amazon Single Sign-On) directory 2092
Amazon IAM Identity Center OIDC service 2104
Amazon Identity and Access Management (IAM) 2106
Amazon Identity and Access Management Roles Anywhere 2143
Amazon Identity Store 2150
Amazon Identity Store Auth 2156
Amazon Identity Sync 2159
Amazon Inspector2 2163
Amazon Invoicing Service 2177
Amazon IoT 2182
Amazon IoT Analytics 2239
Amazon IoT Events 2248
Amazon IoT Greengrass 2256
Amazon IoT Greengrass V2 2279
Amazon IoT Jobs DataPlane 2291
Amazon IoT SiteWise 2294
Amazon IoT TwinMaker 2313
Amazon Key Management Service 2324
Amazon Kinesis Analytics 2389
Amazon Kinesis Analytics V2 2393
Amazon Kinesis Data Streams 2401
Amazon Kinesis Firehose 2412
Amazon Kinesis Video Streams 2417
Amazon Lambda 2426
Amazon Launch Wizard 2444

Amazon License Manager 2452
Amazon License Manager Linux Subscriptions Manager 2463
Amazon Managed Streaming for Apache Kafka 2467
Amazon Managed Workflows for Apache Airflow 2484
Amazon Web Services Marketplace 2490
Amazon Web Services Marketplace Entitlement Service 2497
Amazon Web Services Marketplace Management Portal 2499
Amazon Web Services Marketplace Metering Service 2504
Amazon MemoryDB 2506
Amazon Message Delivery Service 2531
Amazon Message Gateway Service 2535
Amazon MQ 2538
Amazon Neptune 2546
Amazon Network Firewall 2553
Amazon OpenSearch Service 2566
Amazon Organizations 2589
Amazon Payments 2605
Amazon Performance Insights 2612
Amazon Personalize 2617
Amazon Polly 2629
Amazon Price List 2633
Amazon Private Certificate Authority 2635
Amazon Purchase Orders Console 2643
Amazon QuickSight 2649
Amazon RDS 2697
Amazon RDS IAM Authentication 2766
Amazon Recycle Bin 2769
Amazon Redshift 2775
Amazon Redshift Data API 2822
Amazon Redshift Serverless 2828
Amazon Resource Access Manager (RAM) 2847
Amazon Resource Group Tagging API 2866
Amazon Resource Groups 2869
Amazon Route 53 2877
Amazon Route 53 Profiles 2893
Amazon Route 53 Resolver 2899

Amazon S3 2922
Amazon S3 Express 3139
Amazon S3 Glacier 3171
Amazon S3 Object Lambda 3178
Amazon SageMaker 3205
Amazon Savings Plans 3351
Amazon Secrets Manager 3356
Amazon Security Hub 3386
Amazon Security Token Service 3404
Amazon Server Migration Service 3423
Amazon Serverless Application Repository 3430
Service Quotas 3435
Amazon Signer 3444
Amazon Simple Workflow Service 3451
Amazon SimpleDB 3469
Amazon Snowball 3473
Amazon SNS 3479
Amazon SQL Workbench 3489
Amazon SQS 3508
Amazon Step Functions 3514
Amazon Storage Gateway 3525
Amazon Web Services Support 3549
Amazon Systems Manager 3556
Amazon Systems Manager GUI Connect 3600
Amazon Timestream InfluxDB 3603
Amazon Transcribe 3611
Amazon Transfer Family 3625
Amazon Trusted Advisor 3639
Amazon WAF Regional 3650
Amazon WAF V2 3664
Amazon WorkSpaces 3686
Amazon X-Ray 3706
Related resources 3716
Programmatic access to service reference information 3718

Reference

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

Contents

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

Actions, resources, and condition keys for Amazon services

Each Amazon 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 Amazon global condition context keys.
- The **Dependent actions** column includes any additional permissions that you should have, in addition to the permission for the action itself, to successfully call the action. This can be required if the action accesses more than one resource.

  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 Amazon Account Management
- Actions, resources, and condition keys for Apache Kafka APIs for Amazon MSK clusters
- Actions, resources, and condition keys for Amazon API Gateway
- Actions, resources, and condition keys for Amazon API Gateway Management
- Actions, resources, and condition keys for Amazon API Gateway Management V2
- Actions, resources, and condition keys for Amazon App Mesh
- Actions, resources, and condition keys for Amazon AppConfig
- Actions, resources, and condition keys for Amazon Application Auto Scaling
- Actions, resources, and condition keys for Amazon Application Recovery Controller - Zonal Shift
- Actions, resources, and condition keys for Amazon AppSync
- Actions, resources, and condition keys for Amazon Athena
- Actions, resources, and condition keys for Amazon Backup
- Actions, resources, and condition keys for Amazon Backup Gateway
- Actions, resources, and condition keys for Amazon Backup storage

- Actions, resources, and condition keys for Amazon Batch
- Actions, resources, and condition keys for Amazon Billing
- Actions, resources, and condition keys for Amazon Billing Console
- Actions, resources, and condition keys for Amazon Budget Service
- Actions, resources, and condition keys for Amazon Certificate Manager
- Actions, resources, and condition keys for Amazon Web Services Cloud Map
- Actions, resources, and condition keys for Amazon CloudAssist service read write permissions
- Actions, resources, and condition keys for Amazon CloudFormation
- Actions, resources, and condition keys for Amazon CloudFront
- Actions, resources, and condition keys for Amazon CloudTrail
- Actions, resources, and condition keys for Amazon CloudWatch
- Actions, resources, and condition keys for Amazon CloudWatch Application Insights
- Actions, resources, and condition keys for Amazon CloudWatch Logs
- Actions, resources, and condition keys for Amazon CloudWatch Observability Access Manager
- Actions, resources, and condition keys for Amazon CloudWatch Synthetics
- Actions, resources, and condition keys for Amazon CodeBuild
- Actions, resources, and condition keys for Amazon CodeCommit
- Actions, resources, and condition keys for Amazon CodeDeploy
- Actions, resources, and condition keys for Amazon CodeDeploy secure host commands service
- Actions, resources, and condition keys for Amazon CodePipeline
- Actions, resources, and condition keys for Amazon Cognito Identity
- Actions, resources, and condition keys for Amazon Compute Optimizer
- Actions, resources, and condition keys for Amazon Config
- Actions, resources, and condition keys for Amazon Connector Service
- Actions, resources, and condition keys for Amazon Consolidated Billing
- Actions, resources, and condition keys for Amazon Cost and Usage Report
- Actions, resources, and condition keys for Amazon Cost Explorer Service
- Actions, resources, and condition keys for Amazon Data Lifecycle Manager

- Actions, resources, and condition keys for Amazon Database Migration Service
- Actions, resources, and condition keys for Amazon Direct Connect
- Actions, resources, and condition keys for Amazon Directory Service
- Actions, resources, and condition keys for Amazon DynamoDB
- Actions, resources, and condition keys for Amazon DynamoDB Accelerator (DAX)
- 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 EC2 Instance Connect
- Actions, resources, and condition keys for Amazon EKS Auth
- Actions, resources, and condition keys for Amazon Elastic Beanstalk
- 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 Container Service
- 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 Amazon Elastic Load Balancing
- Actions, resources, and condition keys for Amazon Elastic Load Balancing V2
- Actions, resources, and condition keys for Amazon Elastic MapReduce
- Actions, resources, and condition keys for Amazon ElastiCache
- Actions, resources, and condition keys for Amazon Elemental MediaConvert
- Actions, resources, and condition keys for Amazon EMR Serverless
- Actions, resources, and condition keys for Amazon EventBridge
- Actions, resources, and condition keys for Amazon Fapiao Management
- Actions, resources, and condition keys for Amazon Free Tier
- Actions, resources, and condition keys for Amazon FreeRTOS
- Actions, resources, and condition keys for Amazon FSx
- Actions, resources, and condition keys for Amazon GameLift

- Actions, resources, and condition keys for Amazon Glue
- Actions, resources, and condition keys for Amazon Glue DataBrew
- Actions, resources, and condition keys for Amazon GuardDuty
- Actions, resources, and condition keys for Amazon Health APIs and Notifications
- Actions, resources, and condition keys for Amazon IAM Access Analyzer
- Actions, resources, and condition keys for Amazon IAM Identity Center (successor to Amazon Single Sign-On)
- Actions, resources, and condition keys for Amazon IAM Identity Center (successor to Amazon Single Sign-On) directory
- Actions, resources, and condition keys for Amazon IAM Identity Center OIDC service
- Actions, resources, and condition keys for Amazon Identity and Access Management (IAM)
- Actions, resources, and condition keys for Amazon Identity and Access Management Roles Anywhere
- Actions, resources, and condition keys for Amazon Identity Store
- Actions, resources, and condition keys for Amazon Identity Store Auth
- Actions, resources, and condition keys for Amazon Identity Sync
- Actions, resources, and condition keys for Amazon Inspector2
- Actions, resources, and condition keys for Amazon Invoicing Service
- Actions, resources, and condition keys for Amazon IoT
- Actions, resources, and condition keys for Amazon IoT Analytics
- Actions, resources, and condition keys for Amazon IoT Events
- Actions, resources, and condition keys for Amazon IoT Greengrass
- Actions, resources, and condition keys for Amazon IoT Greengrass V2
- Actions, resources, and condition keys for Amazon IoT Jobs DataPlane
- Actions, resources, and condition keys for Amazon IoT SiteWise
- Actions, resources, and condition keys for Amazon IoT TwinMaker
- Actions, resources, and condition keys for Amazon Key Management Service
- Actions, resources, and condition keys for Amazon Kinesis Analytics
- Actions, resources, and condition keys for Amazon Kinesis Analytics V2

- 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 Amazon Kinesis Video Streams
- Actions, resources, and condition keys for Amazon Lambda
- Actions, resources, and condition keys for Amazon Launch Wizard
- Actions, resources, and condition keys for Amazon License Manager
- Actions, resources, and condition keys for Amazon License Manager Linux Subscriptions Manager
- Actions, resources, and condition keys for Amazon Managed Streaming for Apache Kafka
- Actions, resources, and condition keys for Amazon Managed Workflows for Apache Airflow
- Actions, resources, and condition keys for Amazon Web Services Marketplace
- Actions, resources, and condition keys for Amazon Web Services Marketplace Entitlement Service
- Actions, resources, and condition keys for Amazon Web Services Marketplace Management Portal
- Actions, resources, and condition keys for Amazon Web Services Marketplace Metering Service
- Actions, resources, and condition keys for Amazon MemoryDB
- Actions, resources, and condition keys for Amazon Message Delivery Service
- Actions, resources, and condition keys for Amazon Message Gateway Service
- Actions, resources, and condition keys for Amazon MQ
- Actions, resources, and condition keys for Amazon Neptune
- Actions, resources, and condition keys for Amazon Network Firewall
- Actions, resources, and condition keys for Amazon OpenSearch Service
- Actions, resources, and condition keys for Amazon Organizations
- Actions, resources, and condition keys for Amazon Payments
- Actions, resources, and condition keys for Amazon Performance Insights
- Actions, resources, and condition keys for Amazon Personalize
- Actions, resources, and condition keys for Amazon Polly
- Actions, resources, and condition keys for Amazon Price List
- Actions, resources, and condition keys for Amazon Private Certificate Authority
- Actions, resources, and condition keys for Amazon Purchase Orders Console

- Actions, resources, and condition keys for Amazon QuickSight
- Actions, resources, and condition keys for Amazon RDS
- Actions, resources, and condition keys for Amazon RDS IAM Authentication
- Actions, resources, and condition keys for Amazon Recycle Bin
- Actions, resources, and condition keys for Amazon Redshift
- Actions, resources, and condition keys for Amazon Redshift Data API
- Actions, resources, and condition keys for Amazon Redshift Serverless
- Actions, resources, and condition keys for Amazon Resource Access Manager (RAM)
- Actions, resources, and condition keys for Amazon Resource Group Tagging API
- Actions, resources, and condition keys for Amazon Resource Groups
- Actions, resources, and condition keys for Amazon Route 53
- Actions, resources, and condition keys for Amazon Route 53 Profiles
- Actions, resources, and condition keys for Amazon Route 53 Resolver
- Actions, resources, and condition keys for Amazon S3
- Actions, resources, and condition keys for Amazon S3 Express
- Actions, resources, and condition keys for Amazon S3 Glacier
- Actions, resources, and condition keys for Amazon S3 Object Lambda
- Actions, resources, and condition keys for Amazon SageMaker
- Actions, resources, and condition keys for Amazon Savings Plans
- Actions, resources, and condition keys for Amazon Secrets Manager
- Actions, resources, and condition keys for Amazon Security Hub
- Actions, resources, and condition keys for Amazon Security Token Service
- Actions, resources, and condition keys for Amazon Server Migration Service
- Actions, resources, and condition keys for Amazon Serverless Application Repository
- Actions, resources, and condition keys for Service Quotas
- Actions, resources, and condition keys for Amazon Signer
- Actions, resources, and condition keys for Amazon Simple Workflow Service
- Actions, resources, and condition keys for Amazon SimpleDB
- Actions, resources, and condition keys for Amazon Snowball

- Actions, resources, and condition keys for Amazon SNS
- Actions, resources, and condition keys for Amazon SQL Workbench
- Actions, resources, and condition keys for Amazon SQS
- Actions, resources, and condition keys for Amazon Step Functions
- Actions, resources, and condition keys for Amazon Storage Gateway
- Actions, resources, and condition keys for Amazon Web Services Support
- Actions, resources, and condition keys for Amazon Systems Manager
- Actions, resources, and condition keys for Amazon Systems Manager GUI Connect
- Actions, resources, and condition keys for Amazon Timestream InfluxDB
- Actions, resources, and condition keys for Amazon Transcribe
- Actions, resources, and condition keys for Amazon Transfer Family
- Actions, resources, and condition keys for Amazon Trusted Advisor
- Actions, resources, and condition keys for Amazon WAF Regional
- Actions, resources, and condition keys for Amazon WAF V2
- Actions, resources, and condition keys for Amazon WorkSpaces
- Actions, resources, and condition keys for Amazon X-Ray

Actions, resources, and condition keys for Amazon Account Management

Amazon 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 Amazon Account Management

- Resource types defined by Amazon Account Management
- Condition keys for Amazon Account Management

Actions defined by Amazon 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 Amazon. 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.

> **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		
				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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableRegion	Grants permission to enable use of a Region	Write	account		
			accountInOrganization		
				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		

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 Amazon 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 Amazon Account Management

Amazon 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 Amazon 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 Amazon. 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.

> **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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 kafka-cluster:DescribeTopic

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
CreateTopic	Grants permission to create topics on a cluster, equivalent to Apache Kafka's CREATE CLUSTER/TOPIC ACL	Write	topic*		kafka-cluster:Connect

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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
DescribeGroup	Grants permission to describe groups on a cluster, equivalent to Apache Kafka's DESCRIBE GROUP ACL	List	group*		kafka-cluster:Connect

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 Amazon 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 Amazon API Gateway

Amazon API Gateway (service prefix: `execute-api`) 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 API Gateway
- Resource types defined by Amazon API Gateway
- Condition keys for Amazon API Gateway

Actions defined by Amazon API 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 Amazon. 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.

> **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
InvalidateCache	Used to invalidate API cache upon a client request	Write	execute-api-general*		
Invoke	Used to invoke an API upon a client request	Write	execute-api-domain		
			execute-api-general		
ManageConnections	ManageConnections controls access to the @connections API	Write	execute-api-general*		

Resource types defined by Amazon API 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
execute-api-general	`arn:${Partition}:execute-api:${Region}:${Account}:${ApiId}/${Stage}/${Method}/${ApiSpecificResourcePath}`	execute-api:viaDomainArn
execute-api-domain	`arn:${Partition}:execute-api:${Region}:${Account}:/domainnames/${DomainName}+${DomainIdentifier}`	

Condition keys for Amazon API Gateway

Amazon API 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 Amazon global condition context keys.

Condition keys	Description	Type
execute-api:viaDomainArn	Filters access by the domain name ARN the API is called from	String

Actions, resources, and condition keys for Amazon API Gateway Management

Amazon API Gateway Management (service prefix: `apigateway`) 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 API Gateway Management
- Resource types defined by Amazon API Gateway Management
- Condition keys for Amazon API Gateway Management

Actions defined by Amazon API Gateway 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 Amazon. 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.

> **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
AddCertificateToDomain	Grants permission to add certificates for mutual TLS authentication to a domain name. This is an additional authorization control for managing the DomainName resource due to the sensitive nature of mTLS	Permissions management	DomainName		
			DomainNames		
CreateAccessAssociation	Grants permission to create an access association from an access association source to a custom domain name for private APIs	Permissions management	PrivateDomainName		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DELETE	Grants permission to delete a particular resource	Write	ApiKey		
			Authorizer		
			BasePathMapping		
			ClientCertificate		
			Deployment		
			DocumentationPart		
			DocumentationVersion		
			DomainName		
			DomainNameAccessAssociation		
			GatewayResponse		
			Integration		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			IntegrationResponse		
			Method		
			MethodResponse		
			Model		
			PrivateBasePathMapping		
			PrivateDomainName		
			RequestValidator		
			Resource		
			RestApi		
			Stage		
			Tags		
			Template		
			UsagePlan		
			UsagePlanKey		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			VpcLink		
				aws:RequestTag/${TagKey} aws:TagKeys	
GET	Grants permission to read a particular resource	Read	Account		
			ApiKey		
			ApiKeys		
			Authorizer		
			Authorizers		
			BasePathMapping		
			BasePathMappings		
			ClientCertificate		
			ClientCertificates		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Deployment		
			Deployments		
			DocumentationPart		
			DocumentationParts		
			DocumentationVersion		
			DocumentationVersions		
			DomainName		
			DomainNameAccessAssociations		
			DomainNames		
			GatewayResponse		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			GatewayResponses		
			Integration		
			IntegrationResponse		
			Method		
			MethodResponse		
			Model		
			Models		
			PrivateBasePathMapping		
			PrivateBasePathMappings		
			PrivateDomainName		
			RequestValidator		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			RequestValidators		
			Resource		
			Resources		
			RestApi		
			RestApis		
			Sdk		
			Stage		
			Stages		
			Tags		
			UsagePlan		
			UsagePlanKey		
			UsagePlanKeys		
			UsagePlans		
			VpcLink		
			VpcLinks		
PATCH	Grants permission to update a particular resource	Write	Account		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ApiKey		
			Authorizer		
			BasePathMapping		
			ClientCertificate		
			Deployment		
			DocumentationPart		
			DocumentationVersion		
			DomainName		
			GatewayResponse		
			Integration		
			IntegrationResponse		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Method		
			MethodResponse		
			Model		
			PrivateBasePathMapping		
			PrivateDomainName		
			RequestValidator		
			Resource		
			RestApi		
			Stage		
			Template		
			UsagePlan		
			UsagePlanKey		
			VpcLink		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
POST	Grants permission to create a particular resource	Write	ApiKeys		
			Authorizers		
			BasePathMappings		
			ClientCertificates		
			Deployments		
			DocumentationParts		
			DocumentationVersions		
			DomainNameAccessAssociations		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			DomainNames		
			GatewayResponses		
			IntegrationResponse		
			MethodResponse		
			Models		
			PrivateBasePathMappings		
			RequestValidators		
			Resources		
			RestApis		
			Stages		
			UsagePlanKeys		
			UsagePlans		
			VpcLinks		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
PUT	Grants permission to update a particular resource	Write	DocumentationPart		
			GatewayResponse		
			IntegrationResponse		
			MethodResponse		
			RestApi		
			Tags		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RejectAccessAssociation	Grants permission to reject an existing access association owned by another account to a custom domain name for private APIs	Permissions management	PrivateDomainName		
RemoveCertificateFromDomain	Grants permission to remove certificates for mutual TLS authentication from a domain name. This is an additional authorization control for managing the DomainName resource due to the sensitive nature of mTLS	Permissions management	DomainName		
			DomainNames		
SetWebACL	Grants permission to set a WAF access control list (ACL). This is an additional authorization control for managing the Stage resource due to the sensitive nature of WebAcl's	Permissions management	Stage		
			Stages		
UpdateDomainNameManagementPolicy	Grants permission to update the management policy of a custom domain name for private APIs	Permissions management	PrivateDomainName		
UpdateDomainNamePolicy	Grants permission to update the invoke policy of a custom domain name for private APIs	Permissions management	DomainNames		
			PrivateDomainName		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateRestApiPolicy	Grants permission to manage the IAM resource policy for an API. This is an additional authorization control for managing an API due to the sensitive nature of the resource policy	Permissions management	RestApi		
			RestApis		

Resource types defined by Amazon API Gateway 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:${Partition}:apigateway:${Region}::/account`	
ApiKey	`arn:${Partition}:apigateway:${Region}::/apikeys/${ApiKeyId}`	aws:ResourceTag/${TagKey}
ApiKeys	`arn:${Partition}:apigateway:${Region}::/apikeys`	aws:ResourceTag/${TagKey}
Authorizer	`arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/authorizers/${AuthorizerId}`	apigateway:Request/AuthorizerType

Resource types	ARN	Condition keys
		apigateway:Request/AuthorizerUri apigateway:Request/CognitoUserPoolProviderArn apigateway:Resource/AuthorizerType apigateway:Resource/AuthorizerUri apigateway:Resource/CognitoUserPoolProviderArn aws:ResourceTag/${TagKey}
Authorizers	`arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/authorizers`	apigateway:Request/AuthorizerType apigateway:Request/AuthorizerUri apigateway:Request/CognitoUserPoolProviderArn aws:ResourceTag/${TagKey}
BasePathMapping	`arn:${Partition}:apigateway:${Region}::/domainnames/${DomainName}/basepathmappings/${BasePath}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
BasePathMappings	arn:${Partition}:apigateway:${Region}::/domainnames/${DomainName}/basepathmappings	aws:ResourceTag/${TagKey}
ClientCertificate	arn:${Partition}:apigateway:${Region}::/clientcertificates/${ClientCertificateId}	aws:ResourceTag/${TagKey}
ClientCertificates	arn:${Partition}:apigateway:${Region}::/clientcertificates	aws:ResourceTag/${TagKey}
Deployment	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/deployments/${DeploymentId}	aws:ResourceTag/${TagKey}
Deployments	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/deployments	apigateway:Request/StageName aws:ResourceTag/${TagKey}
DocumentationPart	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/documentation/parts/${DocumentationPartId}	aws:ResourceTag/${TagKey}
DocumentationParts	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/documentation/parts	aws:ResourceTag/${TagKey}
DocumentationVersion	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/documentation/versions/${DocumentationVersionId}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
DocumentationVersions	`arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/documentation/versions`	aws:ResourceTag/${TagKey}
DomainName	`arn:${Partition}:apigateway:${Region}::/domainnames/${DomainName}`	apigateway:Request/EndpointType apigateway:Request/MtlsTrustStoreUri apigateway:Request/MtlsTrustStoreVersion apigateway:Request/SecurityPolicy apigateway:Resource/EndpointType apigateway:Resource/MtlsTrustStoreUri apigateway:Resource/MtlsTrustStoreVersion apigateway:Resource/SecurityPolicy aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
DomainNames	arn:${Partition}:apigateway:${Region}::/domainnames	apigateway:Request/EndpointType apigateway:Request/MtlsTrustStoreUri apigateway:Request/MtlsTrustStoreVersion apigateway:Request/SecurityPolicy aws:ResourceTag/${TagKey}
DomainNameAccessAssociation	arn:${Partition}:apigateway:${Region}:${Account}:/domainnameaccessassociations/domainname/${DomainName}/${SourceType}/${SourceId}	
DomainNameAccessAssociations	arn:${Partition}:apigateway:${Region}:${Account}:/domainnameaccessassociations	apigateway:Request/AccessAssociationSource apigateway:Request/DomainNameArn aws:ResourceTag/${TagKey}
GatewayResponse	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/gatewayresponses/${ResponseType}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
GatewayResponses	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/gatewayresponses	aws:ResourceTag/${TagKey}
Integration	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/resources/${ResourceId}/methods/${HttpMethodType}/integration	aws:ResourceTag/${TagKey}
IntegrationResponse	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/resources/${ResourceId}/methods/${HttpMethodType}/integration/responses/${StatusCode}	aws:ResourceTag/${TagKey}
Method	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/resources/${ResourceId}/methods/${HttpMethodType}	apigateway:Request/ApiKeyRequired apigateway:Request/RouteAuthorizationType apigateway:Resource/ApiKeyRequired apigateway:Resource/RouteAuthorizationType aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
MethodResponse	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/resources/${ResourceId}/methods/${HttpMethodType}/responses/${StatusCode}	aws:ResourceTag/${TagKey}
Model	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/models/${ModelName}	aws:ResourceTag/${TagKey}
Models	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/models	aws:ResourceTag/${TagKey}
PrivateBasePathMapping	arn:${Partition}:apigateway:${Region}::/domainnames/${DomainName}+${DomainIdentifier}/basepathmappings/${BasePath}	aws:ResourceTag/${TagKey}
PrivateBasePathMappings	arn:${Partition}:apigateway:${Region}::/domainnames/${DomainName}+${DomainIdentifier}/basepathmappings	aws:ResourceTag/${TagKey}
PrivateDomainName	arn:${Partition}:apigateway:${Region}:${Account}:/domainnames/${DomainName}+${DomainIdentifier}	apigateway:Request/EndpointType apigateway:Resource/EndpointType aws:ResourceTag/${TagKey}
RequestValidator	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/requestvalidators/${RequestValidatorId}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
RequestValidators	`arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/requestvalidators`	aws:ResourceTag/${TagKey}
Resource	`arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/resources/${ResourceId}`	aws:ResourceTag/${TagKey}
Resources	`arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/resources`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
RestApi	`arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}`	apigateway:Request/ApiKeyRequired apigateway:Request/ApiName apigateway:Request/AuthorizerType apigateway:Request/AuthorizerUri apigateway:Request/DisableExecuteApiEndpoint apigateway:Request/EndpointType apigateway:Request/RouteAuthorizationType apigateway:Resource/ApiKeyRequired apigateway:Resource/ApiName apigateway:Resource/AuthorizerType apigateway:Resource/AuthorizerUri

Resource types	ARN	Condition keys
		apigateway:Resource/DisableExecuteApiEndpoint apigateway:Resource/EndpointType apigateway:Resource/RouteAuthorizationType aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
RestApis	`arn:${Partition}:apigateway:${Region}::/restapis`	apigateway:Request/ApiKeyRequired apigateway:Request/ApiName apigateway:Request/AuthorizerType apigateway:Request/AuthorizerUri apigateway:Request/DisableExecuteApiEndpoint apigateway:Request/EndpointType apigateway:Request/RouteAuthorizationType aws:ResourceTag/${TagKey}
Sdk	`arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/stages/${StageName}/sdks/${SdkType}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
Stage	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/stages/${StageName}	apigateway:Request/AccessLoggingDestination apigateway:Request/AccessLoggingFormat apigateway:Resource/AccessLoggingDestination apigateway:Resource/AccessLoggingFormat aws:ResourceTag/${TagKey}
Stages	arn:${Partition}:apigateway:${Region}::/restapis/${RestApiId}/stages	apigateway:Request/AccessLoggingDestination apigateway:Request/AccessLoggingFormat aws:ResourceTag/${TagKey}
Template	arn:${Partition}:apigateway:${Region}::/restapis/models/${ModelName}/template	aws:ResourceTag/${TagKey}
UsagePlan	arn:${Partition}:apigateway:${Region}::/usageplans/${UsagePlanId}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
UsagePlans	`arn:${Partition}:apigateway:${Region}::/usageplans`	aws:ResourceTag/${TagKey}
UsagePlanKey	`arn:${Partition}:apigateway:${Region}::/usageplans/${UsagePlanId}/keys/${Id}`	aws:ResourceTag/${TagKey}
UsagePlanKeys	`arn:${Partition}:apigateway:${Region}::/usageplans/${UsagePlanId}/keys`	aws:ResourceTag/${TagKey}
VpcLink	`arn:${Partition}:apigateway:${Region}::/vpclinks/${VpcLinkId}`	aws:ResourceTag/${TagKey}
VpcLinks	`arn:${Partition}:apigateway:${Region}::/vpclinks`	aws:ResourceTag/${TagKey}
Tags	`arn:${Partition}:apigateway:${Region}::/tags/${UrlEncodedResourceARN}`	

Condition keys for Amazon API Gateway Management

Amazon API Gateway 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 Amazon global condition context keys.

Condition keys	Description	Type
apigateway:Request/AccessAssociationSource	Filters access by access association source. Available during the CreateDomainNameAccessAssociation operation	String

Condition keys	Description	Type
apigateway:Request/AccessLoggingDestination	Filters access by access log destination. Available during the CreateStage and UpdateStage operations	String
apigateway:Request/AccessLoggingFormat	Filters access by access log format. Available during the CreateStage and UpdateStage operations	String
apigateway:Request/ApiKeyRequired	Filters access by whether an API key is required or not. Available during the CreateMethod and PutMethod operations. Also available as a collection during import and reimport	ArrayOfBool
apigateway:Request/ApiName	Filters access by API name. Available during the CreateRestApi and UpdateRestApi operations	String
apigateway:Request/AuthorizerType	Filters access by type of authorizer in the request, for example TOKEN, REQUEST, JWT. Available during CreateAuthorizer and UpdateAuthorizer. Also available during import and reimport as an ArrayOfString	ArrayOfString
apigateway:Request/AuthorizerUri	Filters access by URI of a Lambda authorizer function. Available during CreateAuthorizer and UpdateAuthorizer. Also available during import and reimport as an ArrayOfString	ArrayOfString
apigateway:Request/CognitoUserPoolProviderArn	Filters access by Cognito user pool provider ARN. Available during CreateAuthorizer and UpdateAuthorizer	ARN

Condition keys	Description	Type
apigateway:Request/DisableExecuteApiEndpoint	Filters access by status of the default execute-api endpoint. Available during the CreateRestApi and DeleteRestApi operations	Bool
apigateway:Request/DomainNameArn	Filters access by domain name ARN. Available during the CreateDomainNameAccessAssociation operation	ARN
apigateway:Request/EndpointType	Filters access by endpoint type. Available during the CreateDomainName, UpdateDomainName, CreateRestApi, and UpdateRestApi operations	ArrayOfString
apigateway:Request/MtlsTrustStoreUri	Filters access by URI of the truststore used for mutual TLS authentication. Available during the CreateDomainName and UpdateDomainName operations	String
apigateway:Request/MtlsTrustStoreVersion	Filters access by version of the truststore used for mutual TLS authentication. Available during the CreateDomainName and UpdateDomainName operations	String
apigateway:Request/RouteAuthorizationType	Filters access by authorization type, for example NONE, AWS_IAM, CUSTOM, JWT, COGNITO_USER_POOLS. Available during the CreateMethod and PutMethod operations Also available as a collection during import	ArrayOfString
apigateway:Request/SecurityPolicy	Filters access by TLS version. Available during the CreateDomain and UpdateDomain operations	ArrayOfString

Condition keys	Description	Type
apigateway:Request/StageName	Filters access by stage name of the deployment that you attempt to create. Available during the CreateDeployment operation	String
apigateway:Resource/AccessLoggingDestination	Filters access by access log destination of the current Stage resource. Available during the UpdateStage and DeleteStage operations	String
apigateway:Resource/AccessLoggingFormat	Filters access by access log format of the current Stage resource. Available during the UpdateStage and DeleteStage operations	String
apigateway:Resource/ApiKeyRequired	Filters access by whether an API key is required or not for the existing Method resource. Available during the PutMethod and DeleteMethod operations. Also available as a collection during reimport	ArrayOfBool
apigateway:Resource/ApiName	Filters access by API name of the existing RestApi resource. Available during UpdateRestApi and DeleteRestApi operations	String
apigateway:Resource/AuthorizerType	Filters access by the current type of authorizer, for example TOKEN, REQUEST, JWT. Available during UpdateAuthorizer and DeleteAuthorizer operations. Also available during reimport as an ArrayOfString	ArrayOfString
apigateway:Resource/AuthorizerUri	Filters access by URI of a Lambda authorizer function. Available during UpdateAuthorizer and DeleteAuthorizer operations. Also available during reimport as an ArrayOfString	ArrayOfString

Condition keys	Description	Type
apigateway:Resource/CognitoUserPoolProviderArn	Filters access by Cognito user pool provider ARN. Available during CreateAuthorizer and UpdateAuthorizer	ARN
apigateway:Resource/DisableExecuteApiEndpoint	Filters access by status of the default execute-api endpoint of the current RestApi resource. Available during UpdateRestApi and DeleteRestApi operations	Bool
apigateway:Resource/EndpointType	Filters access by endpoint type. Available during the UpdateDomainName, DeleteDomainName, UpdateRestApi, and DeleteRestApi operations	ArrayOfString
apigateway:Resource/MtlsTrustStoreUri	Filters access by URI of the truststore used for mutual TLS authentication. Available during UpdateDomainName and DeleteDomainName operations	String
apigateway:Resource/MtlsTrustStoreVersion	Filters access by version of the truststore used for mutual TLS authentication. Available during UpdateDomainName and DeleteDomainName operations	String
apigateway:Resource/RouteAuthorizationType	Filters access by authorization type of the existing Method resource, for example NONE, AWS_IAM, CUSTOM, JWT, COGNITO_USER_POOLS. Available during the PutMethod and DeleteMethod operations. Also available as a collection during reimport	ArrayOfString
apigateway:Resource/SecurityPolicy	Filters access by TLS version. Available during UpdateDomain and DeleteDomain operations	ArrayOfString

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 the request	ArrayOfString

Actions, resources, and condition keys for Amazon API Gateway Management V2

Amazon API Gateway Management V2 (service prefix: `apigateway`) 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 API Gateway Management V2
- Resource types defined by Amazon API Gateway Management V2
- Condition keys for Amazon API Gateway Management V2

Actions defined by Amazon API Gateway Management 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 Amazon. 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.

> **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
DELETE	Grants permission to delete a particular resource	Write	AccessLogSettings		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Api		
			ApiMapping		
			Authorizer		
			AuthorizersCache		
			Cors		
			Deployment		
			Integration		
			IntegrationResponse		
			Model		
			Route		
			RouteRequestParameter		
			RouteResponse		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			RouteSettings		
			Stage		
			VpcLink		
				aws:RequestTag/${TagKey} aws:TagKeys	
GET	Grants permission to read a particular resource	Read	AccessLogSettings		
			Api		
			ApiMapping		
			ApiMappings		
			Apis		
			Authorizer		
			Authorizers		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			AuthorizersCache		
			Cors		
			Deployment		
			Deployments		
			ExportedAPI		
			Integration		
			IntegrationResponse		
			IntegrationResponses		
			Integrations		
			Model		
			ModelTemplate		
			Models		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Route		
			RouteRequestParameter		
			RouteResponse		
			RouteResponses		
			RouteSettings		
			Routes		
			Stage		
			Stages		
			VpcLink		
			VpcLinks		
PATCH	Grants permission to update a particular resource	Write	Api		
			ApiMapping		
			Authorizer		
			Deployment		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Integration		
			IntegrationResponse		
			Model		
			Route		
			RouteRequestParameter		
			RouteResponse		
			Stage		
			VpcLink		
				aws:RequestTag/${TagKey} aws:TagKeys	
POST	Grants permission to create a particular resource	Write	ApiMappings		
			Apis		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Authorizers		
			Deployments		
			IntegrationResponses		
			Integrations		
			Models		
			RouteResponses		
			Routes		
			Stages		
			VpcLinks		
				aws:RequestTag/${TagKey} aws:TagKeys	
PUT	Grants permission to update a particular resource	Write	Api		
			Apis		

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

Resource types defined by Amazon API Gateway Management 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
AccessLogSettings	`arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/stages/${StageName}/accesslogsettings`	aws:ResourceTag/${TagKey}
Api	`arn:${Partition}:apigateway:${Region}::/apis/${ApiId}`	apigateway:Request/ApiKeyRequired apigateway:Request/ApiName apigateway:Request/AuthorizerType

Resource types	ARN	Condition keys
		apigateway:Request/AuthorizerUri apigateway:Request/DisableExecuteApiEndpoint apigateway:Request/EndpointType apigateway:Request/RouteAuthorizationType apigateway:Resource/ApiKeyRequired apigateway:Resource/ApiName apigateway:Resource/AuthorizerType apigateway:Resource/AuthorizerUri apigateway:Resource/DisableExecuteApiEndpoint apigateway:Resource/EndpointType apigateway:Resource/RouteAuthorizationType

Resource types	ARN	Condition keys
		aws:ResourceTag/${TagKey}
Apis	arn:${Partition}:apigateway:${Region}::/apis	apigateway:Request/ApiKeyRequired apigateway:Request/ApiName apigateway:Request/AuthorizerType apigateway:Request/AuthorizerUri apigateway:Request/DisableExecuteApiEndpoint apigateway:Request/EndpointType apigateway:Request/RouteAuthorizationType aws:ResourceTag/${TagKey}
ApiMapping	arn:${Partition}:apigateway:${Region}::/domainnames/${DomainName}/apimappings/${ApiMappingId}	aws:ResourceTag/${TagKey}
ApiMappings	arn:${Partition}:apigateway:${Region}::/domainnames/${DomainName}/apimappings	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
Authorizer	`arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/authorizers/${AuthorizerId}`	apigateway:Request/AuthorizerType apigateway:Request/AuthorizerUri apigateway:Resource/AuthorizerType apigateway:Resource/AuthorizerUri aws:ResourceTag/${TagKey}
Authorizers	`arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/authorizers`	apigateway:Request/AuthorizerType apigateway:Request/AuthorizerUri aws:ResourceTag/${TagKey}
AuthorizersCache	`arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/stages/${StageName}/cache/authorizers`	aws:ResourceTag/${TagKey}
Cors	`arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/cors`	aws:ResourceTag/${TagKey}
Deployment	`arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/deployments/${DeploymentId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
Deployments	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/deployments	apigateway:Request/StageName aws:ResourceTag/${TagKey}
ExportedAPI	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/exports/${Specification}	aws:ResourceTag/${TagKey}
Integration	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/integrations/${IntegrationId}	aws:ResourceTag/${TagKey}
Integrations	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/integrations	aws:ResourceTag/${TagKey}
IntegrationResponse	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/integrations/${IntegrationId}/integrationresponses/${IntegrationResponseId}	aws:ResourceTag/${TagKey}
IntegrationResponses	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/integrations/${IntegrationId}/integrationresponses	aws:ResourceTag/${TagKey}
Model	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/models/${ModelId}	aws:ResourceTag/${TagKey}
Models	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/models	aws:ResourceTag/${TagKey}
ModelTemplate	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/models/${ModelId}/template	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
Route	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/routes/${RouteId}	apigateway:Request/ApiKeyRequired apigateway:Request/RouteAuthorizationType apigateway:Resource/ApiKeyRequired apigateway:Resource/RouteAuthorizationType aws:ResourceTag/${TagKey}
Routes	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/routes	apigateway:Request/ApiKeyRequired apigateway:Request/RouteAuthorizationType aws:ResourceTag/${TagKey}
RouteResponse	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/routes/${RouteId}/routeresponses/${RouteResponseId}	aws:ResourceTag/${TagKey}
RouteResponses	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/routes/${RouteId}/routeresponses	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
RouteRequestParameter	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/routes/${RouteId}/requestparameters/${RequestParameterKey}	aws:ResourceTag/${TagKey}
RouteSettings	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/stages/${StageName}/routesettings/${RouteKey}	aws:ResourceTag/${TagKey}
Stage	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/stages/${StageName}	apigateway:Request/AccessLoggingDestination apigateway:Request/AccessLoggingFormat apigateway:Resource/AccessLoggingDestination apigateway:Resource/AccessLoggingFormat aws:ResourceTag/${TagKey}
Stages	arn:${Partition}:apigateway:${Region}::/apis/${ApiId}/stages	apigateway:Request/AccessLoggingDestination apigateway:Request/AccessLoggingFormat aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
VpcLink	`arn:${Partition}:apigateway:${Region}::/vpclinks/${VpcLinkId}`	aws:ResourceTag/${TagKey}
VpcLinks	`arn:${Partition}:apigateway:${Region}::/vpclinks`	aws:ResourceTag/${TagKey}

Condition keys for Amazon API Gateway Management V2

Amazon API Gateway Management 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 Amazon global condition context keys.

Condition keys	Description	Type
apigateway:Request/AccessLoggingDestination	Filters access by access log destination. Available during the CreateStage and UpdateStage operations	String
apigateway:Request/AccessLoggingFormat	Filters access by access log format. Available during the CreateStage and UpdateStage operations	String
apigateway:Request/ApiKeyRequired	Filters access by the requirement of API. Available during the CreateRoute and UpdateRoute operations. Also available as a collection during import and reimport	ArrayOfBool

Condition keys	Description	Type
apigateway:Request/ApiName	Filters access by API name. Available during the CreateApi and UpdateApi operations	String
apigateway:Request/AuthorizerType	Filters access by type of authorizer in the request, for example REQUEST or JWT. Available during CreateAuthorizer and UpdateAuthorizer. Also available during import and reimport as an ArrayOfString	ArrayOfString
apigateway:Request/AuthorizerUri	Filters access by URI of a Lambda authorizer function. Available during CreateAuthorizer and UpdateAuthorizer. Also available during import and reimport as an ArrayOfString	ArrayOfString
apigateway:Request/DisableExecuteApiEndpoint	Filters access by status of the default execute-api endpoint. Available during the CreateApi and UpdateApi operations	Bool
apigateway:Request/EndpointType	Filters access by endpoint type. Available during the CreateDomainName, UpdateDomainName, CreateApi, and UpdateApi operations	ArrayOfString
apigateway:Request/MtlsTrustStoreUri	Filters access by URI of the truststore used for mutual TLS authentication. Available during the CreateDomainName and UpdateDomainName operations	String
apigateway:Request/MtlsTrustStoreVersion	Filters access by version of the truststore used for mutual TLS authentication. Available during the CreateDomainName and UpdateDomainName operations	String

Condition keys	Description	Type
apigateway:Request/RouteAuthorizationType	Filters access by authorization type, for example NONE, AWS_IAM, CUSTOM, JWT. Available during the CreateRoute and UpdateRoute operations. Also available as a collection during import	ArrayOfString
apigateway:Request/SecurityPolicy	Filters access by TLS version. Available during the CreateDomain and UpdateDomain operations	ArrayOfString
apigateway:Request/StageName	Filters access by stage name of the deployment that you attempt to create. Available during the CreateDeployment operation	String
apigateway:Resource/AccessLoggingDestination	Filters access by access log destination of the current Stage resource. Available during the UpdateStage and DeleteStage operations	String
apigateway:Resource/AccessLoggingFormat	Filters access by access log format of the current Stage resource. Available during the UpdateStage and DeleteStage operations	String
apigateway:Resource/ApiKeyRequired	Filters access by the requirement of API key for the existing Route resource. Available during the UpdateRoute and DeleteRoute operations. Also available as a collection during reimport	ArrayOfBool
apigateway:Resource/ApiName	Filters access by API name. Available during the UpdateApi and DeleteApi operations	String

Condition keys	Description	Type
apigateway:Resource/AuthorizerType	Filters access by the current type of authorizer, for example REQUEST or JWT. Available during UpdateAuthorizer and DeleteAuthorizer operations. Also available during import and reimport as an ArrayOfString	ArrayOfString
apigateway:Resource/AuthorizerUri	Filters access by the URI of the current Lambda authorizer associated with the current API. Available during UpdateAuthorizer and DeleteAuthorizer. Also available as a collection during reimport	ArrayOfString
apigateway:Resource/DisableExecuteApiEndpoint	Filters access by status of the default execute-api endpoint. Available during the UpdateApi and DeleteApi operations	Bool
apigateway:Resource/EndpointType	Filters access by endpoint type. Available during the UpdateDomainName, DeleteDomainName, UpdateApi, and DeleteApi operations	ArrayOfString
apigateway:Resource/MtlsTrustStoreUri	Filters access by URI of the truststore used for mutual TLS authentication. Available during the UpdateDomainName and DeleteDomainName operations	String
apigateway:Resource/MtlsTrustStoreVersion	Filters access by version of the truststore used for mutual TLS authentication. Available during the UpdateDomainName and DeleteDomainName operations	String
apigateway:Resource/RouteAuthorizationType	Filters access by authorization type of the existing Route resource, for example NONE, AWS_IAM, CUSTOM. Available during the UpdateRoute and DeleteRoute operations. Also available as a collection during reimport	ArrayOfString

Condition keys	Description	Type
apigateway:Resource/SecurityPolicy	Filters access by TLS version. Available during the UpdateDomainName and DeleteDomainName operations	ArrayOfString
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 App Mesh

Amazon App Mesh (service prefix: `appmesh`) 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 App Mesh
- Resource types defined by Amazon App Mesh
- Condition keys for Amazon App Mesh

Actions defined by Amazon App Mesh

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 Amazon. 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.

> **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
CreateGatewayRoute	Grants permission to create a gateway route that is associated with a virtual gateway	Write	gatewayRoute*	aws:TagKeys aws:RequestTag/${TagKey}	
			virtualService		
CreateMesh	Grants permission to create a service mesh	Write	mesh*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateRoute	Grants permission to create a route that is associated with a virtual router	Write	route*	aws:TagKeys aws:RequestTag/${TagKey}	
			virtualNode		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateVirtualGateway	Grants permission to create a virtual gateway within a service mesh	Write	virtualGateway*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateVirtualNode	Grants permission to create a virtual node within a service mesh	Write	virtualNode*	aws:TagKeys aws:RequestTag/${TagKey}	
			virtualService		
CreateVirtualRouter	Grants permission to create a virtual router within a service mesh	Write	virtualRouter*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateVirtualService	Grants permission to create a virtual service within a service mesh	Write	virtualService*	aws:TagKeys aws:RequestTag/${TagKey}	
			virtualNode		
			virtualRouter		
DeleteGatewayRoute	Grants permission to delete an existing gateway route	Write	gatewayRoute*		
DeleteMesh	Grants permission to delete an existing service mesh	Write	mesh*		
DeleteMeshPolicy [permission only]	Grants permission to delete the RAM access control policy for a mesh	Write	mesh*		
DeleteRoute	Grants permission to delete an existing route	Write	route*		
DeleteVirtualGateway	Grants permission to delete an existing virtual gateway	Write	virtualGateway*		
DeleteVirtualNode	Grants permission to delete an existing virtual node	Write	virtualNode*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVirtualRouter	Grants permission to delete an existing virtual router	Write	virtualRouter*		
DeleteVirtualService	Grants permission to delete an existing virtual service	Write	virtualService*		
DescribeGatewayRoute	Grants permission to describe an existing gateway route	Read	gatewayRoute*		
DescribeMesh	Grants permission to describe an existing service mesh	Read	mesh*		
DescribeRoute	Grants permission to describe an existing route	Read	route*		
DescribeVirtualGateway	Grants permission to describe an existing virtual gateway	Read	virtualGateway*		
DescribeVirtualNode	Grants permission to describe an existing virtual node	Read	virtualNode*		
DescribeVirtualRouter	Grants permission to describe an existing virtual router	Read	virtualRouter*		
DescribeVirtualService	Grants permission to describe an existing virtual service	Read	virtualService*		
GetMeshPolicy [permission only]	Grants permission to read the RAM access control policy for a mesh	Read	mesh*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListGatewayRoutes	Grants permission to list existing gateway routes in a service mesh	List	virtualGateway*		
ListMeshes	Grants permission to list existing service meshes	List			
ListRoutes	Grants permission to list existing routes in a service mesh	List	virtualRouter*		
ListTagsForResource	Grants permission to list the tags for an App Mesh resource	List	gatewayRoute		
			mesh		
			route		
			virtualGateway		
			virtualNode		
			virtualRouter		
			virtualService		
ListVirtualGateways	Grants permission to list existing virtual gateways in a service mesh	List	mesh*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListVirtualNodes	Grants permission to list existing virtual nodes	List	mesh*		
ListVirtualRouters	Grants permission to list existing virtual routers in a service mesh	List	mesh*		
ListVirtualServices	Grants permission to list existing virtual services in a service mesh	List	mesh*		
PutMeshPolicy [permission only]	Grants permission to define the RAM access control policy for a mesh	Write	mesh*		
StreamAggregatedResources	Grants permission to receive streamed resources for an App Mesh endpoint (VirtualNode/VirtualGateway)	Read	virtualGateway		
			virtualNode		
TagResource	Grants permission to tag a resource with a specified resourceArn	Tagging	gatewayRoute		
			mesh		
			route		
			virtualGateway		
			virtualNode		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			virtualRouter		
			virtualService		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to delete a tag from a resource	Tagging	gatewayRoute		
			mesh		
			route		
			virtualGateway		
			virtualNode		
			virtualRouter		
			virtualService		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
UpdateGatewayRoute	Grants permission to update an existing gateway route for a specified service mesh and virtual gateway	Write	gatewayRoute*		
			virtualService		
UpdateMesh	Grants permission to update an existing service mesh	Write	mesh*		
UpdateRoute	Grants permission to update an existing route for a specified service mesh and virtual router	Write	route*		
			virtualNode		
UpdateVirtualGateway	Grants permission to update an existing virtual gateway in a specified service mesh	Write	virtualGateway*		
UpdateVirtualNode	Grants permission to update an existing virtual node in a specified service mesh	Write	virtualNode*		
UpdateVirtualRouter	Grants permission to update an existing virtual router in a specified service mesh	Write	virtualRouter*		
UpdateVirtualService	Grants permission to update an existing virtual service in a specified service mesh	Write	virtualService*		
			virtualNode		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			virtualRouter		

Resource types defined by Amazon App Mesh

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
mesh	`arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}`	aws:ResourceTag/${TagKey}
virtualService	`arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualService/${VirtualServiceName}`	aws:ResourceTag/${TagKey}
virtualNode	`arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualNode/${VirtualNodeName}`	aws:ResourceTag/${TagKey}
virtualRouter	`arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualRouter/${VirtualRouterName}`	aws:ResourceTag/${TagKey}
route	`arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualRo`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
	uter/${VirtualRouterName}/route/${RouteName}	
virtualGateway	arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualGateway/${VirtualGatewayName}	aws:ResourceTag/${TagKey}
gatewayRoute	arn:${Partition}:appmesh:${Region}:${Account}:mesh/${MeshName}/virtualGateway/${VirtualGatewayName}/gatewayRoute/${GatewayRouteName}	aws:ResourceTag/${TagKey}

Condition keys for Amazon App Mesh

Amazon App Mesh 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 Amazon global condition context keys.

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

Actions, resources, and condition keys for Amazon AppConfig

Amazon 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 Amazon AppConfig
- Resource types defined by Amazon AppConfig
- Condition keys for Amazon AppConfig

Actions defined by Amazon 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 Amazon. 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.

> **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/${TagKey} aws:TagKeys	
CreateConfigurationProfile	Grants permission to create a configuration profile	Write	application*		
				aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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 Amazon 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 Amazon AppConfig

Amazon 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 Amazon 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 Amazon 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 Auto Scaling

Amazon Application Auto Scaling (service prefix: `application-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 Application Auto Scaling
- Resource types defined by Amazon Application Auto Scaling
- Condition keys for Amazon Application Auto Scaling

Actions defined by Amazon Application 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 Amazon. 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.

> **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
DeleteScalingPolicy	Grants permission to delete a scaling policy	Write	ScalableTarget*		
				application-autoscaling:service-namespace application-autosc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aling:scalable-dimension	
DeleteScheduledAction	Grants permission to delete a scheduled action	Write	ScalableTarget*		
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
DeregisterScalableTarget	Grants permission to deregister a scalable target	Write	ScalableTarget*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
DescribeScalableTargets	Grants permission to describe one or more scalable targets in the specified namespace	Read			
DescribeScalingActivities	Grants permission to describe a set of scaling activities or all scaling activities in the specified namespace	Read			
DescribeScalingPolicies	Grants permission to describe a set of scaling policies or all scaling policies in the specified namespace	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeScheduledActions	Grants permission to describe a set of scheduled actions or all scheduled actions in the specified namespace	Read			
GetPredictiveScalingForecast	Grants permission to retrieve the forecast data for a predictive scaling policy	List			
ListTagsForResource	Grants permission to list tags for a scalable target	Read	ScalableTarget*		
PutScalingPolicy	Grants permission to create and update a scaling policy for a scalable target	Write	ScalableTarget*		
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutScheduledAction	Grants permission to create and update a scheduled action for a scalable target	Write	ScalableTarget*		
				application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
RegisterScalableTarget	Grants permission to register Amazon or custom resources as scalable targets with Application Auto Scaling and to update configuration parameters used to manage a scalable target	Write	ScalableTarget*		application-autoscaling:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys application-autoscaling:service-namespace application-autoscaling:scalable-dimension	
TagResource	Grants permission to tag a scalable target	Tagging	ScalableTarget*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from a scalable target	Tagging	ScalableTarget*		
				aws:TagKeys	

Resource types defined by Amazon Application 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
ScalableTarget	`arn:${Partition}:application-autoscaling:${Region}:${Account}:scalable-target/${ResourceId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Application Auto Scaling

Amazon Application 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 Amazon global condition context keys.

Condition keys	Description	Type
application-autoscaling:scalable-dimension	Filters access by the scalable dimension that is passed in the request	String
application-autoscaling:service-namespace	Filters access by the service namespace that is passed in the request	String
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 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 Amazon. 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.

> **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
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			
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* 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 Amazon 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 Amazon AppSync

Amazon AppSync (service prefix: `appsync`) 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 AppSync
- Resource types defined by Amazon AppSync
- Condition keys for Amazon AppSync

Actions defined by Amazon AppSync

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 Amazon. 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.

> **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
AssociateApi	Grants permission to attach a GraphQL API to a custom domain name in AppSync	Write	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateMergedGraphqlApi	Grants permission to associate a merged API to a source API	Write	graphqlapi*		
AssociateSourceGraphqlApi	Grants permission to associate a source API to a merged API	Write	graphqlapi*		
CreateApi	Grants permission to create an API	Write		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole
CreateApiCache	Grants permission to create an API cache in AppSync	Write			
CreateApiKey	Grants permission to create a unique key that you can distribute to clients who are executing your API	Write			
CreateChannelNamespace	Grants permission to create a channel namespace	Write	channelNamespace*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSource	Grants permission to create a data source	Write			
CreateDomainName	Grants permission to create a custom domain name in AppSync	Write		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateFunction	Grants permission to create a new function	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateGraphqlApi	Grants permission to create a GraphQL API, which is the top level AppSync resource	Write		aws:RequestTag/${TagKey} aws:TagKeys appsync:Visibility	iam:CreateServiceLinkedRole
CreateResolver	Grants permission to create a resolver. A resolver converts incoming requests into a format that a data source can understand, and converts the data source's responses into GraphQL	Write			
CreateType	Grants permission to create a type	Write			
DeleteApi	Grants permission to delete a API. This will also clean up every AppSync resource below that API	Write	api*		
				aws:ResourceTag/${TagKey}	
DeleteApiCache	Grants permission to delete an API cache in AppSync	Write			
DeleteApiKey	Grants permission to delete an API key	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteChannelNamespace	Grants permission to delete a channel namespace	Write	channelNamespace*		
				aws:ResourceTag/${TagKey}	
DeleteDataSource	Grants permission to delete a data source	Write			
DeleteDomainName	Grants permission to delete a custom domain name in AppSync	Write	domain*		
				aws:ResourceTag/${TagKey}	
DeleteFunction	Grants permission to delete a function	Write			
DeleteGraphqlApi	Grants permission to delete a GraphQL Api. This will also clean up every AppSync resource below that API	Write	graphqlapi*		
				aws:ResourceTag/${TagKey}	
DeleteResolver	Grants permission to delete a resolver	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteResourcePolicy [permission only]	Grants permission to remove a resource policy	Write			
DeleteType	Grants permission to delete a type	Write			
DisassociateApi	Grants permission to detach a GraphQL API to a custom domain name in AppSync	Write	domain*		
DisassociateMergedGraphqlApi	Grants permission to remove an associated source API from a merged API identified by the source API	Write	mergedApiAssociation*		
DisassociateSourceGraphqlApi	Grants permission to remove an associated source API from a merged API identified by the merged API	Write	sourceApiAssociation*		
EvaluateCode	Grants permission to evaluate code with a runtime and context	Read			
EvaluateMappingTemplate	Grants permission to evaluate template mapping	Read			
EventConnect	Grants permission to connect to an Event API	Write	api*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EventPublish	Grants permission to publish events to a channel namespace	Write	channelNamespace*		
EventSubscribe	Grants permission to subscribe to a channel namespace	Write	channelNamespace*		
FlushApiCache	Grants permission to flush an API cache in AppSync	Write			
GetApi	Grants permission to retrieve an API	Read	api*		
				aws:ResourceTag/${TagKey}	
GetApiAssociation	Grants permission to read custom domain name - GraphQL API association details in AppSync	Read	domain*		
GetApiCache	Grants permission to read information about an API cache in AppSync	Read			
GetChannelNamespace	Grants permission to retrieve a channel namespace	Read	channelNamespace*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDataSource	Grants permission to retrieve a data source	Read			
GetDataSourceIntrospection	Grants permission to retrieve a data source introspection	Read			
GetDomainName	Grants permission to read information about a custom domain name in AppSync	Read	domain*		
				aws:ResourceTag/${TagKey}	
GetFunction	Grants permission to retrieve a function	Read			
GetGraphqlApi	Grants permission to retrieve a GraphQL API	Read	graphqlapi*		
				aws:ResourceTag/${TagKey}	
GetGraphqlApiEnvironmentVariables	Grants permission to retrieve the environment variables for a GraphQL API	Read			
GetIntrospectionSchema	Grants permission to retrieve the introspection schema for a GraphQL API	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetResolver	Grants permission to retrieve a resolver	Read			
GetResourcePolicy [permission only]	Grants permission to read a resource policy	Read			
GetSchemaCreationStatus	Grants permission to retrieve the current status of a schema creation operation	Read			
GetSourceApiAssociation	Grants permission to read information about a merged API associated source API	Read	sourceApiAssociation*		
GetType	Grants permission to retrieve a type	Read			
GraphQL [permission only]	Grants permission to send a GraphQL query to a GraphQL API	Write	field*		
			graphqlapi*		
ListApiKeys	Grants permission to list the API keys for a given API	List			
ListApis	Grants permission to list APIs	List		aws:ResourceTag/${TagKey}	
	Grants permission to list channel namespace	List	api*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListChannelNamespaces				aws:ResourceTag/${TagKey}	
ListDataSources	Grants permission to list the data sources for a given API	List			
ListDomainNames	Grants permission to enumerate custom domain names in AppSync	List		aws:ResourceTag/${TagKey}	
ListFunctions	Grants permission to list the functions for a given API	List			
ListGraphqlApis	Grants permission to list GraphQL APIs	List			
ListResolvers	Grants permission to list the resolvers for a given API and type	List			
ListResolversByFunction	Grants permission to list the resolvers that are associated with a specific function	List			
ListSourceApiAssociations	Grants permission to list source APIs associated to a given merged API	List			
ListTagsForResource	Grants permission to list the tags for a resource	Read	api		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			channelNamespace		
			domain		
			graphqlapi		
				aws:ResourceTag/${TagKey}	
ListTypes	Grants permission to list the types for a given API	List			
ListTypesByAssociation	Grants permission to list the types for a given merged API and source API association	List			
PutGraphqlApiEnvironmentVariables	Grants permission to update the environment variables for a GraphQL API	Write			
PutResourcePolicy [permission only]	Grants permission to set a resource policy	Write			
SetWebACL	Grants permission to set a web ACL	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SourceGraphQL [permission only]	Grants permission to send a GraphQL query to a source API of a merged API	Write	field*		
			graphqlapi*		
StartDataSourceIntrospection	Grants permission to introspect a data source	Write			
StartSchemaCreation	Grants permission to add a new schema to your GraphQL API. This operation is asynchronous - GetSchemaCreationStatus can show when it has completed	Write			
StartSchemaMerge	Grants permission to initiate a schema merge for a given merged API and associated source API	Write	sourceApiAssociation*		
TagResource	Grants permission to tag a resource	Tagging	api		
			channelNamespace		
			domain		
			graphqlapi		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a resource	Tagging	api		
			channelNamespace		
			domain		
			graphqlapi		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateApi	Grants permission to update an API	Write	api*		iam:CreateServiceLinkedRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
UpdateApiCache	Grants permission to update an API cache in AppSync	Write			
UpdateApiKey	Grants permission to update an API key for a given API	Write			
UpdateChannelNamespace	Grants permission to update a channel namespace	Write	channelNamespace*		
				aws:ResourceTag/${TagKey}	
UpdateDataSource	Grants permission to update a data source	Write			
UpdateDomainName	Grants permission to update a custom domain name in AppSync	Write	domain*		
				aws:ResourceTag/${TagKey}	
UpdateFunction	Grants permission to update an existing function	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateGraphqlApi	Grants permission to update a GraphQL API	Write	graphqlapi*		iam:CreateServiceLinkedRole
				aws:ResourceTag/${TagKey}	
UpdateResolver	Grants permission to update a resolver	Write			
UpdateSourceApiAssociation	Grants permission to update a merged API source API association	Write	sourceApiAssociation*		
UpdateType	Grants permission to update a type	Write			

Resource types defined by Amazon AppSync

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
datasource	arn:${Partition}:appsync:${Region}:${Account}:apis/${GraphQLAPIId}/datasources/${DatasourceName}	
domain	arn:${Partition}:appsync:${Region}:${Account}:domainnames/${DomainName}	aws:ResourceTag/${TagKey}
graphqlapi	arn:${Partition}:appsync:${Region}:${Account}:apis/${GraphQLAPIId}	aws:ResourceTag/${TagKey}
field	arn:${Partition}:appsync:${Region}:${Account}:apis/${GraphQLAPIId}/types/${TypeName}/fields/${FieldName}	
type	arn:${Partition}:appsync:${Region}:${Account}:apis/${GraphQLAPIId}/types/${TypeName}	
function	arn:${Partition}:appsync:${Region}:${Account}:apis/${GraphQLAPIId}/functions/${FunctionId}	
sourceApiAssociation	arn:${Partition}:appsync:${Region}:${Account}:apis/${MergedGraphQLAPIId}/sourceApiAssociations/${Associationid}	
mergedApiAssociation	arn:${Partition}:appsync:${Region}:${Account}:apis/${SourceGraphQLAPIId}/mergedApiAssociations/${Associationid}	
api	arn:${Partition}:appsync:${Region}:${Account}:apis/${ApiId}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
channelNamespace	`arn:${Partition}:appsync:${Region}:${Account}:apis/${ApiId}/channelNamespace/${ChannelNamespaceName}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon AppSync

Amazon AppSync 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 Amazon global condition context keys.

Condition keys	Description	Type
appsync:Visibility	Filters access by the visibility of an API	String
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 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 Athena

Amazon Athena (service prefix: `athena`) 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 Athena
- Resource types defined by Amazon Athena
- Condition keys for Amazon Athena

Actions defined by Amazon Athena

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 Amazon. 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.

> **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
BatchGetNamedQuery	Grants permission to get information about one or more named queries	Read	workgroup*		
BatchGetPreparedStatement	Grants permission to get information about one or more prepared statements	Read	workgroup*		
BatchGetQueryExecution	Grants permission to get information about one or more query executions	Read	workgroup*		
CancelCapacityReservation	Grants permission to cancel a capacity reservation	Write	capacity-reservation*		
CancelQueryExecution	Grants permission to cancel query execution. Deprecated. Applies only to Amazon services and principals that use Athena JDBC driver earlier than 1.1.0. Use StopQueryExecution otherwise	Write	workgroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCapacityReservation	Grants permission to create a capacity reservation	Write	capacity-reservation*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataCatalog	Grants permission to create a datacatalog	Write	datacatalog*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNamedQuery	Grants permission to create a named query	Write	workgroup*		
CreateNotebook	Grants permission to create a notebook	Write	workgroup*		
CreatePreparedStatement	Grants permission to create a prepared statement	Write	workgroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePresignedNotebookUrl	Grants permission to create a presigned notebook url	Write	workgroup*		
CreateWorkGroup	Grants permission to create a workgroup	Write	workgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCapacityReservation	Grants permission to delete a capacity reservation	Write	capacity-reservation*		
DeleteDataCatalog	Grants permission to delete a datacatalog	Write	datacatalog*		
DeleteNamedQuery	Grants permission to delete a named query specified	Write	workgroup*		
DeleteNotebook	Grants permission to delete a notebook	Write	workgroup*		
DeletePreparedStatement	Grants permission to delete a prepared statement specified	Write	workgroup*		
DeleteWorkGroup	Grants permission to delete a workgroup	Write	workgroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ExportNotebook	Grants permission to export a notebook	Write	workgroup*		
GetCalculationExecution	Grants permission to get a calculation execution	Read	workgroup*		
GetCalculationExecutionCode	Grants permission to get a calculation execution code	Read	workgroup*		
GetCalculationExecutionStatus	Grants permission to get a calculation execution status	Read	workgroup*		
GetCapacityAssignmentConfiguration	Grants permission to get capacity assignment information for a capacity reservation	Read	capacity-reservation*		
GetCapacityReservation	Grants permission to get a capacity reservation	Read	capacity-reservation*		
GetCatalogs	Grants permission to enable access to databases and tables. Applies only to Amazon services managed policy and principals that use an Athena JDBC driver version 1.1.0	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDataCatalog	Grants permission to get a datacatalog	Read	datacatalog*		
GetDatabase	Grants permission to get a database for a given datacatalog	Read	datacatalog*		
GetExecutionEngine	Grants permission to enable access to the specified database and table. Applies only to Amazon services managed policy and principals that use an Athena JDBC driver version 1.1.0	Read			
GetExecutionEngines	Grants permission to enable access to databases and tables. Applies only to Amazon services managed policy and principals that use an Athena JDBC driver version 1.1.0	Read			
GetNamedQuery	Grants permission to get information about the specified named query	Read	workgroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetNamespace	Grants permission to enable access to the specified database and table. Applies only to Amazon services managed policy and principals that use an Athena JDBC driver version 1.1.0	Read			
GetNamespaces	Grants permission to enable access to databases and tables. Applies only to Amazon services managed policy and principals that use an Athena JDBC driver version 1.1.0	Read			
GetNotebookMetadata	Grants permission to get notebook metadata	Read	workgroup*		
GetPreparedStatement	Grants permission to get information about the specified prepared statement	Read	workgroup*		
GetQueryExecution	Grants permission to get information about the specified query execution	Read	workgroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetQueryExecutions	Grants permission to get query executions. Deprecated. Applies only to Amazon services and principals that use Athena JDBC driver earlier than 1.1.0. Use ListQueryExecutions otherwise	Read			
GetQueryResults	Grants permission to get the query results	Read	workgroup*		
GetQueryResultsStream	Grants permission to get the query results stream	Read	workgroup*		
GetQueryRuntimeStatistics	Grants permission to get runtime statistics for the specified query execution	Read	workgroup*		
GetSession	Grants permission to get a session	Read	workgroup*		
GetSessionStatus	Grants permission to get a session status	Read	workgroup*		
GetTable	Grants permission to enable access to the specified table. Applies only to Amazon services managed policy and principals that use an Athena JDBC driver version 1.1.0	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTableMetadata	Grants permission to get a metadata about a table for a given datacatalog	Read	datacatalog*		
GetTables	Grants permission to enable access to tables. Applies only to Amazon services managed policy and principals that use an Athena JDBC driver version 1.1.0	Read			
GetWorkGroup	Grants permission to get a workgroup	Read	workgroup*		
ImportNotebook	Grants permission to import a notebook	Write	workgroup*		
ListApplicationDPUSizes	Grants permission to return a list of ApplicationRuntimeIds	List			
ListCalculationExecutions	Grants permission to return a list of calculation executions	List	workgroup*		
ListCapacityReservations	Grants permission to return a list of capacity reservations for the specified Amazon Web Services account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDataCatalogs	Grants permission to return a list of datacatalogs for the specified Amazon Web Services account	List			
ListDatabases	Grants permission to return a list of databases for a given datacatalog	List	datacatalog*		
ListEngineVersions	Grants permission to return a list of athena engine versions for the specified Amazon Web Services account	Read			
ListExecutors	Grants permission to return a list of executors	List			
ListNamedQueries	Grants permission to return a list of named queries in Amazon Athena for the specified Amazon Web Services account	List	workgroup*		
ListNotebookMetadata	Grants permission to return a list of notebooks for a given workgroup	List	workgroup*		
ListNotebookSessions	Grants permission to return a list of sessions for a given notebook	List	workgroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPreparedStatements	Grants permission to return a list of prepared statements for the specified workgroup	List	workgroup*		
ListQueryExecutions	Grants permission to return a list of query executions for the specified Amazon Web Services account	Read	workgroup*		
ListSessions	Grants permission to return a list of sessions for a given workgroup	List	workgroup*		
ListTableMetadata	Grants permission to return a list of table metadata in a database for a given datacatalog	Read	datacatalog*		
ListTagsForResource	Grants permission to return a list of tags for a resource	Read	capacity-reservation*		
			datacatalog*		
			workgroup*		
ListWorkGroups	Grants permission to return a list of workgroups for the specified Amazon Web Services account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutCapacityAssignmentConfiguration	Grants permission to assign capacity from a capacity reservation to queries	Write	capacity-reservation*		
			workgroup*		
RunQuery	Grants permission to run a query. Deprecated. Applies only to Amazon services and principals that use Athena JDBC driver earlier than 1.1.0. Use StartQueryExecution otherwise	Write			
StartCalculationExecution	Grants permission to start a calculation execution	Write	workgroup*		
StartQueryExecution	Grants permission to start a query execution using an SQL query provided as a string	Write	workgroup*		
StartSession	Grants permission to start a session	Write	workgroup*		
StopCalculationExecution	Grants permission to stop a calculation execution	Write	workgroup*		
StopQueryExecution	Grants permission to stop the specified query execution	Write	workgroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to add a tag to a resource	Tagging	capacity-reservation*		
			datacatalog*		
			workgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
TerminateSession	Grants permission to terminate a session	Write	workgroup*		
UntagResource	Grants permission to remove a tag from a resource	Tagging	capacity-reservation*		
			datacatalog*		
			workgroup*		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateCapacityReservation	Grants permission to update a capacity reservation	Write	capacity-reservation*		
UpdateDataCatalog	Grants permission to update a datacatalog	Write	datacatalog*		
UpdateNamedQuery	Grants permission to update a named query specified	Write	workgroup*		
UpdateNotebook	Grants permission to update a notebook	Write	workgroup*		
UpdateNotebookMetadata	Grants permission to update notebook metadata	Write	workgroup*		
UpdatePreparedStatement	Grants permission to update a prepared statement	Write	workgroup*		
UpdateWorkGroup	Grants permission to update a workgroup	Write	workgroup*		

Resource types defined by Amazon Athena

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
datacatalog	`arn:${Partition}:athena:${Region}:${Account}:datacatalog/${DataCatalogName}`	aws:ResourceTag/${TagKey}
workgroup	`arn:${Partition}:athena:${Region}:${Account}:workgroup/${WorkGroupName}`	aws:ResourceTag/${TagKey}
capacity-reservation	`arn:${Partition}:athena:${Region}:${Account}:capacity-reservation/${CapacityReservationName}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Athena

Amazon Athena 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 Amazon 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 the tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Backup

Amazon 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 Amazon Backup
- Resource types defined by Amazon Backup
- Condition keys for Amazon Backup

Actions defined by Amazon 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 Amazon. 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.

> **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
CancelLegalHold	Grants permission to cancel a legal hold	Write	legalHold*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey}	
CreateBackupPlan	Grants permission to create a new backup plan	Write	backupPlan*		
				aws:RequestTag/${TagKey} aws:TagKeys	
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLegalHold	Grants permission to create a new legal hold	Write	legalHold*		
				aws:RequestTag/${TagKey} aws:TagKeys	

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRestoreTestingPlan	Grants permission to create a new restore testing plan	Write	restoreTestingPlan*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRestoreTestingSelection	Grants permission to create a new resource assignment in a restore testing plan	Write	restoreTestingPlan*		iam:PassRole
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*		
DeleteBackupVaultAccessPolicy	Grants permission to delete backup vault access policy	Permissions management	backupVault*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
DeleteRestoreTestingSelection	Grants permission to delete a resource assignment from a restore testing plan	Write	restoreTestingPlan*		

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeRestoreJob	Grants permission to describe a restore job	Read			
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetBackupVaultNotifications	Grants permission to get backup vault notifications	Read	backupVault*		
GetBackupVaultSharingPolicy [permission only]	Grants permission to get backup vault sharing policy	Read	backupVault*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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 Amazon 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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListBackupVaults	Grants permission to list backup vaults	List			
ListCopyJobSummaries	Grants permission to list copy job summaries	List			
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 Amazon Backup	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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			
ListRestoreJobSummaries	Grants permission to list restore job summaries	List			
ListRestoreJobs	Grants permission to list restore jobs	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListRestoreJobsByProtectedResource	Grants permission to list restore jobs for a protected resource	List			
ListRestoreTestingPlans	Grants permission to list restore testing plans	List			
ListRestoreTestingSelections	Grants permission to list resource assignments for a specific restore testing plan	List	restoreTestingPlan*		
ListTags	Grants permission to list tags for a resource	Read	backupPlan		
			backupVault		
			framework		
			legalHold		
			recoveryPoint		
			reportPlan		
			restoreTestingPlan		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
PutRestoreValidationResult	Grants permission to put a restore validation result	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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
StopBackupJob	Grants permission to stop a backup job	Write			
TagResource	Grants permission to tag a resource	Tagging	backupPlan		
			backupVault		
			framework		
			legalHold		
			recoveryPoint		

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
UpdateBackupPlan	Grants permission to update a backup plan	Write	backupPlan*		
UpdateFramework	Grants permission to update a framework	Write	framework*		
UpdateGlobalSettings	Grants permission to update the current global settings for the Amazon Account	Write			
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	

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

Resource types defined by Amazon 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}

Resource types	ARN	Condition keys
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}

Condition keys for Amazon Backup

Amazon 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 Amazon 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

Condition keys	Description	Type
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
backup:CopyTargets	Filters access by the ARN of an 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

Actions, resources, and condition keys for Amazon Backup Gateway

Amazon Backup Gateway (service prefix: `backup-gateway`) 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 Backup Gateway
- Resource types defined by Amazon Backup Gateway
- Condition keys for Amazon Backup Gateway

Actions defined by Amazon Backup 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 Amazon. 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.

> **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
AssociateGatewayToServer	Grants permission to AssociateGatewayToServer	Write	gateway*		
			hypervisor*		
Backup	Grants permission to Backup	Write	virtualmachine*		
CreateGateway	Grants permission to to CreateGateway	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteGateway	Grants permission to DeleteGateway	Write	gateway*		
DeleteHypervisor	Grants permission to DeleteHypervisor	Write	hypervisor*		
DisassociateGatewayFromServer	Grants permission to DisassociateGatewayFromServer	Write	gateway*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetBandwidthRateLimitSchedule	Grants permission to GetBandwidthRateLimitSchedule	Read	gateway*		
GetGateway	Grants permission to GetGateway	Read	gateway*		
GetHypervisor	Grants permission to GetHypervisor	Read	hypervisor*		
GetHypervisorPropertyMappings	Grants permission to GetHypervisorPropertyMappings	Read	hypervisor*		
GetVirtualMachine	Grants permission to GetVirtualMachine	Read	virtualmachine*		
ImportHypervisorConfiguration	Grants permission to ImportHypervisorConfiguration	Write		aws:RequestTag/${TagKey} aws:TagKeys	
ListGateways	Grants permission to ListGateways	Read			
ListHypervisors	Grants permission to ListHypervisors	Read			
ListTagsForResource	Grants permission to ListTagsForResource	Read	gateway		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			hypervisor		
			virtualmachine		
ListVirtualMachines	Grants permission to ListVirtualMachines	Read			
PutBandwidthRateLimitSchedule	Grants permission to PutBandwidthRateLimitSchedule	Write	gateway*		
PutHypervisorPropertyMappings	Grants permission to PutHypervisorPropertyMappings	Write	hypervisor*		iam:PassRole
PutMaintenanceStartTime	Grants permission to PutMaintenanceStartTime	Write	gateway*		
Restore	Grants permission to Restore	Write	hypervisor*		
StartVirtualMachinesMetadataSync	Grants permission to StartVirtualMachinesMetadataSync	Write	hypervisor*		iam:PassRole
TagResource	Grants permission to TagResource	Tagging	gateway		
			hypervisor		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			virtualmachine		
				aws:RequestTag/${TagKey} aws:TagKeys	
TestHypervisorConfiguration	Grants permission to TestHypervisorConfiguration	Write	gateway*		
UntagResource	Grants permission to UntagResource	Tagging	gateway		
			hypervisor		
			virtualmachine		
				aws:TagKeys	
UpdateGatewayInformation	Grants permission to UpdateGatewayInformation	Write	gateway*		
UpdateGatewaySoftwareNow	Grants permission to UpdateGatewaySoftwareNow	Write	gateway*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateHypervisor	Grants permission to UpdateHypervisor	Write	gateway*		

Resource types defined by Amazon Backup 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
gateway	`arn:${Partition}:backup-gateway:${Region}:${Account}:gateway/${GatewayId}`	aws:ResourceTag/${TagKey}
hypervisor	`arn:${Partition}:backup-gateway:${Region}:${Account}:hypervisor/${HypervisorId}`	aws:ResourceTag/${TagKey}
virtualmachine	`arn:${Partition}:backup-gateway:${Region}:${Account}:vm/${VirtualmachineId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Backup Gateway

Amazon Backup 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 Amazon 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 Amazon Backup storage

Amazon Backup storage (service prefix: `backup-storage`) 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 Backup storage
- Resource types defined by Amazon Backup storage
- Condition keys for Amazon Backup storage

Actions defined by Amazon Backup storage

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 Amazon. 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.

> **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
CommitBackupJob [permission only]	Grants permission to commit backup job	Write			
DeleteObjects [permission only]	Grants permission to delete objects	Write			
DescribeBackupJob [permission only]	Grants permission to describe backup job	Write			
GetBaseBackup [permission only]	Grants permission to get base backup	Write			
GetChunk [permission only]	Grants permission to get data from a recovery point for a restore job	Write			
GetIncrementalBaseBackup [permission only]	Grants permission to get incremental base backup	Write			
GetObjectMetadata [permission only]	Grants permission to get metadata from a recovery point for a restore job	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListChunks [permission only]	Grants permission to list data from a recovery point for a restore job	Write			
ListObjects [permission only]	Grants permission to list data from a recovery point for a restore job	Write			
MountCapsule [permission only]	Associates a KMS key to a backup vault	Write			
NotifyObjectComplete [permission only]	Grants permission to mark an uploaded data as completed for a backup job	Write			
PutChunk [permission only]	Grants permission to upload data to an Amazon Backup-managed recovery point for a backup job	Write			
PutObject [permission only]	Grants permission to put object	Write			
StartObject [permission only]	Grants permission to upload data to an Amazon Backup-managed recovery point for a backup job	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateObjectComplete [permission only]	Grants permission to update object complete	Write			

Resource types defined by Amazon Backup storage

Amazon Backup storage does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon Backup storage, specify `"Resource": "*"` in your policy.

Condition keys for Amazon Backup storage

Backup Storage 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 Amazon global condition context keys.

Actions, resources, and condition keys for Amazon Batch

Amazon 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 Amazon Batch
- Resource types defined by Amazon Batch
- Condition keys for Amazon Batch

Actions defined by Amazon 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 Amazon. 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.

> **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 Amazon Batch job queue in your account	Write	job*		
CreateComputeEnvironment	Grants permission to create an Amazon Batch compute environment in your account	Write	compute-environment*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateConsumableResource	Grants permission to create an Amazon Batch consumable resource in your account	Write	consumable-resource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateJobQueue	Grants permission to create an Amazon Batch job queue in your account	Write	compute-environment*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			job-queue*	aws:RequestTag/${TagKey} aws:TagKeys	
			scheduling-policy		
CreateSchedulingPolicy	Grants permission to create an Amazon Batch scheduling policy in your account	Write	scheduling-policy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteComputeEnvironment	Grants permission to delete an Amazon Batch compute environment in your account	Write	compute-environment*		
DeleteConsumableResource	Grants permission to delete an Amazon Batch consumable resource in your account	Write	consumable-resource*		
DeleteJobQueue	Grants permission to delete an Amazon 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 Amazon Batch scheduling policy in your account	Write	scheduling-policy*		
DeregisterJobDefinition	Grants permission to deregister an Amazon Batch job definition in your account	Write	job-definition-revision*		
DescribeComputeEnvironments	Grants permission to describe one or more Amazon Batch compute environments in your account	Read			
DescribeConsumableResource	Grants permission to describe one or more Amazon Batch consumable resource in your account	Read	consumable-resource*		
DescribeJobDefinitions	Grants permission to describe one or more Amazon Batch job definitions in your account	Read			
DescribeJobQueues	Grants permission to describe one or more Amazon Batch job queues in your account	Read			
DescribeJobs	Grants permission to describe a list of Amazon Batch jobs in your account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeScheduling Policies	Grants permission to describe one or more Amazon Batch scheduling policies in your account	Read			
GetJobQueueSnapshot	Grants permission to get a snapshot of an Amazon Batch job queue in your account	Read	job-queue*		
ListConsumableResources	Grants permission to list Amazon Batch consumable resources in your account	List			
ListJobs	Grants permission to list jobs for a specified Amazon Batch job queue in your account	List			
ListJobsByConsumableResource	Grants permission to list Amazon Batch jobs that require a specific consumable resource in your account	List	consumable-resource*		
ListSchedulingPolicies	Grants permission to list Amazon Batch scheduling policies in your account	Read			
ListTagsForResource	Grants permission to list tags for an Amazon Batch resource in your account	Read	compute-environment		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			consumable-resource		
			job		
			job-definition-revision		
			job-queue		
			scheduling-policy		
RegisterJobDefinition	Grants permission to register an Amazon Batch job definition in your account	Write	job-definition*		
			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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SubmitJob	Grants permission to submit an Amazon Batch job from a job definition in your account	Write	job*	batch:ShareIdentifier batch:EKSImage batch:EKSNamespace aws:RequestTag/${TagKey} aws:TagKeys	
			job-definition*		
			job-queue*		
			consumable-resource		
TagResource	Grants permission to tag an Amazon Batch resource in your account	Tagging	compute-environment		

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

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

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

Resource types defined by Amazon 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}

Resource types	ARN	Condition keys
job-definition	arn:${Partition}:batch:${Region}:${Account}:job-definition/${JobDefinitionName}	
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}
consumable-resource	arn:${Partition}:batch:${Region}:${Account}:consumable-resource/${ConsumableResourceName}	aws:ResourceTag/${TagKey}

Condition keys for Amazon Batch

Amazon 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 Amazon 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 Billing

Amazon Billing (service prefix: `billing`) 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 Billing
- Resource types defined by Amazon Billing
- Condition keys for Amazon Billing

Actions defined by Amazon Billing

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 Amazon. 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.

> **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
CreateBillingView	Grants permission to create a billing view	Write	billingview*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteBillingView	Grants permission to delete a billing view	Write	billingview*		
				aws:ResourceTag/${TagKey}	
DeleteResourcePolicy [permission only]	Grants permission to delete a billing view resource policy	Permissions management	billingview*		
				aws:ResourceTag/${TagKey}	
GetBillingData [permission only]	Grants permission to perform queries on billing information	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetBillingDetails [permission only]	Grants permission to view detailed line item billing information	Read			
GetBillingNotifications [permission only]	Grants permission to view notifications sent by Amazon related to your accounts billing information	Read			
GetBillingPreferences [permission only]	Grants permission to view billing preferences such as reserved instance, savings plans and credits sharing	Read			
GetBillingView	Grants permission to get the metadata for a specified billing view	Read	billingview*		
				aws:ResourceTag/${TagKey}	
GetContractInformation [permission only]	Grants permission to view the account's contract information including the contract number, end-user organization names, PO numbers and if the account is used to service public-sector customers	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCredits [permission only]	Grants permission to view credits that have been redeemed	Read			
GetIAMAccessPreference [permission only]	Grants permission to retrieve the state of the Allow IAM Access billing preference	Read			
GetResourcePolicy	Grants permission to get the resource policy specified billing view	Permissions management	billingview*		
				aws:ResourceTag/${TagKey}	
GetSellerOfRecord [permission only]	Grants permission to retrieve the account's default Seller of Record	Read			
ListBillingViews	Grants permission to get a list of all your available billing views	Read			
ListSourceViewsForBillingView	Grants permission to get the list of source views for a specified billing view	List	billingview*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
ListTagsForResource	Grants permission to get the list of tags for a specified billing view	Read	billingview*		
				aws:ResourceTag/${TagKey}	
PutContractInformation [permission only]	Grants permission to set the account's contract information end-user organization names and if the account is used to service public-sector customers	Write			
PutResourcePolicy [permission only]	Grants permission to put a billing view resource policy	Permissions management	billingview*		
				aws:ResourceTag/${TagKey}	
RedeemCredits [permission only]	Grants permission to redeem an Amazon credit	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to add tags to a specified billing view	Tagging	billingview*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to remove a tag from a specified billing view	Tagging	billingview*		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateBillingPreferences [permission only]	Grants permission to update billing preferences such as reserved instance, savings plans and credits sharing	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateBillingView	Grants permission to update a billing view	Write	billingview*		
				aws:ResourceTag/${TagKey}	
UpdateIAMAccessPreference [permission only]	Grants permission to update the Allow IAM Access billing preference	Write			

Resource types defined by Amazon Billing

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
billingview	`arn:${Partition}:billing::${Account}:billingview/${ResourceId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Billing

Amazon Billing 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 Amazon 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 Billing Console

Amazon Billing Console (service prefix: `aws-portal`) 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 Billing Console
- Resource types defined by Amazon Billing Console
- Condition keys for Amazon Billing Console

Actions defined by Amazon Billing 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 Amazon. 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.

> **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
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			
ModifyAccount [permission only]	Allow or deny IAM users permission to modify Account Settings	Write			
ModifyBilling [permission only]	Allow or deny IAM users permission to modify billing settings	Write			
ModifyPaymentMethods [permission only]	Allow or deny IAM users permission to modify payment methods	Write			
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			
ViewAccount [permission only]	Allow or deny IAM users permission to view account settings	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ViewBilling [permission only]	Allow or deny IAM users permission to view billing pages in the console	Read			
ViewPaymentMethods [permission only]	Allow or deny IAM users permission to view payment methods	Read			
ViewUsage [permission only]	Allow or deny IAM users permission to view Amazon usage reports	Read			

Resource types defined by Amazon Billing Console

Amazon Billing Console does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon Billing Console, specify `"Resource": "*"` in your policy.

Condition keys for Amazon Billing Console

Billing 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 Amazon global condition context keys.

Actions, resources, and condition keys for Amazon Budget Service

Amazon 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 Amazon Budget Service
- Resource types defined by Amazon Budget Service
- Condition keys for Amazon Budget Service

Actions defined by Amazon 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 Amazon. 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.

> **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 Amazon 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 threshold. Creating a budget action with tags also requires the 'budgets:TagResource' permission	Write	budgetAction*		iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove resource tags from a budget or budget action	Tagging	budget		
			budgetAction		
				aws:TagKeys	

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

Resource types defined by Amazon 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}

Resource types	ARN	Condition keys
		aws:TagKeys

Condition keys for Amazon Budget Service

Amazon 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 Amazon 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

Actions, resources, and condition keys for Amazon Certificate Manager

Amazon 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 Amazon Certificate Manager
- Resource types defined by Amazon Certificate Manager
- Condition keys for Amazon Certificate Manager

Actions defined by Amazon 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 Amazon. 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.

> **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*		
				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 a private certificate issued by a private certificate authority (CA) for use anywhere	Read	certificate*		
GetAccountConfiguration	Grants permission to retrieve account level configuration from Amazon Certificate Manager	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 Amazon Certificate Manager (ACM)	Write	certificate*		
				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 Amazon Certificate Manager	Write			
RemoveTagsFromCertificate	Grants permission to remove one or more tags from a certificate	Tagging	certificate*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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	
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
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 Amazon 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 Amazon Certificate Manager

Amazon 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 Amazon 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: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 Amazon Web Services Cloud Map

Amazon Web Services Cloud Map (service prefix: `servicediscovery`) 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 Web Services Cloud Map
- Resource types defined by Amazon Web Services Cloud Map
- Condition keys for Amazon Web Services Cloud Map

Actions defined by Amazon Web Services Cloud Map

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 Amazon. 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.

> **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
CreateHttpNamespace	Grants permission to create an HTTP namespace	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreatePrivateDnsNamespace	Grants permission to create a private namespace based on DNS, which will be visible only inside a specified Amazon VPC	Write		aws:TagKeys aws:RequestTag/${TagKey}	
CreatePublicDnsNamespace	Grants permission to create a public namespace based on DNS, which will be visible on the internet	Write		aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateService	Grants permission to create a service	Write	namespace*		
			service*		
				servicediscovery:NamespaceArn aws:TagKeys aws:RequestTag/${TagKey}	
DeleteNamespace	Grants permission to delete a specified namespace	Write	namespace*		
DeleteService	Grants permission to delete a specified service	Write	service*		
DeleteServiceAttributes	Grants permission to delete specified attributes from a service	Write	service*		
DeregisterInstance	Grants permission to delete the records and the health check, if any, that Amazon Route 53 created for the specified instance	Write	service*		
				servicediscovery:ServiceArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DiscoverInstances	Grants permission to discover registered instances for a specified namespace and service	Read		servicediscovery:NamespaceName servicediscovery:ServiceName	
DiscoverInstancesRevision	Grants permission to discover the revision of the instances for a specified namespace and service	Read		servicediscovery:NamespaceName servicediscovery:ServiceName	
GetInstance	Grants permission to get information about a specified instance	Read		servicediscovery:ServiceArn	
GetInstancesHealthStatus	Grants permission to get the current health status (Healthy, Unhealthy, or Unknown) of one or more instances	Read		servicediscovery:ServiceArn	
GetNamespace	Grants permission to get information about a namespace	Read	namespace*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetOperation	Grants permission to get information about a specific operation	Read			
GetService	Grants permission to get the settings for a specified service	Read	service*		
GetServiceAttributes	Grants permission to get the attributes for a specified service	Read	service*		
ListInstances	Grants permission to get summary information about the instances that were registered with a specified service	Read		servicediscovery:ServiceArn	
ListNamespaces	Grants permission to get information about the namespaces	Read			
ListOperations	Grants permission to list operations that match the criteria that you specify	List			
ListServices	Grants permission to get settings for all the services that match specified filters	Read			
ListTagsForResource	Grants permission to lists tags for the specified resource	Read			
RegisterInstance		Write	service*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to register an instance based on the settings in a specified service			servicediscovery:ServiceArn	
TagResource	Grants permission to add one or more tags to the specified resource	Tagging		aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove one or more tags from the specified resource	Tagging		aws:TagKeys	
UpdateHttpNamespace	Grants permission to update the settings for a HTTP namespace	Write	namespace*		
UpdateInstanceCustomHealthStatus	Grants permission to update the current health status for an instance that has a custom health check	Write		servicediscovery:ServiceArn	
UpdatePrivateDnsNamespace	Grants permission to update the settings for a private DNS namespace	Write	namespace*		
UpdatePublicDnsNamespace	Grants permission to update the settings for a public DNS namespace	Write	namespace*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateService	Grants permission to update the settings in a specified service	Write	service*		
UpdateServiceAttributes	Grants permission to update the attributes in a specified service	Write	service*		

Resource types defined by Amazon Web Services Cloud Map

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
namespace	`arn:${Partition}:servicediscovery:${Region}:${Account}:namespace/${NamespaceId}`	aws:ResourceTag/${TagKey}
service	`arn:${Partition}:servicediscovery:${Region}:${Account}:service/${ServiceId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Web Services Cloud Map

Amazon Web Services Cloud Map 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 Amazon global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters actions based on the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters actions based on the tags associated with the resource	String
aws:TagKeys	Filters actions based on the tag keys that are passed in the request	ArrayOfString
servicediscovery:NamespaceArn	Filters access by specifying the Amazon Resource Name (ARN) for the related namespace	ARN
servicediscovery:NamespaceName	Filters access by specifying the name of the related namespace	String
servicediscovery:ServiceArn	Filters access by specifying the Amazon Resource Name (ARN) for the related service	ARN
servicediscovery:ServiceName	Filters access by specifying the name of the related service	String

Actions, resources, and condition keys for Amazon CloudAssist service read write permissions

Amazon CloudAssist service read write permissions (service prefix: `cloudassist`) 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 CloudAssist service read write permissions
- Resource types defined by Amazon CloudAssist service read write permissions
- Condition keys for Amazon CloudAssist service read write permissions

Actions defined by Amazon CloudAssist service read write permissions

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 Amazon. 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.

> **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
DescribeAccountRealNameInformation	Grants permission to get account real name information	Read			
UpdateAccountRealNameInformation	Grants permission to update account real name information	Write			

Resource types defined by Amazon CloudAssist service read write permissions

Amazon CloudAssist service read write permissions does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon CloudAssist service read write permissions, specify `"Resource": "*"` in your policy.

Condition keys for Amazon CloudAssist service read write permissions

CloudAssist 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 Amazon global condition context keys.

Actions, resources, and condition keys for Amazon CloudFormation

Amazon CloudFormation (service prefix: `cloudformation`) 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 CloudFormation
- Resource types defined by Amazon CloudFormation
- Condition keys for Amazon CloudFormation

Actions defined by Amazon CloudFormation

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 Amazon. 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.

> **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
ActivateOrganizationsAccess	Grants permission to activate trusted access between StackSets and Organizations. With trusted access between StackSets and Organizations	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	activated, the management account has permissions to create and manage StackSets for your organization				
ActivateType	Grants permission to activate a public third-party extension , making it available for use in stack templates	Write			
BatchDescribeTypeConfigurations	Grants permission to return configuration data for the specified CloudFormation extensions	Read			
CancelUpdateStack	Grants permission to cancel an update on the specified stack	Write	stack*		
ContinueUpdateRollback	Grants permission to continue rolling back a stack that is in the UPDATE_ROLLBACK_FAILED state to the UPDATE_ROLLBACK_COMPLETE state	Write	stack*		
				cloudformation:RoleArn	
CreateChangeSet	Grants permission to create a list of changes for a stack	Write	stack*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				cloudformation:ChangeSetName cloudformation:ResourceTypes cloudformation:ImportResourceTypes cloudformation:RoleArn cloudformation:StackPolicyUrl cloudformation:TemplateUrl aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
CreateGeneratedTemplate	Grants permission to create a template from existing resources that are not already managed with CloudFormation	Write			
CreateStack	Grants permission to create a stack as specified in the template	Write	stack*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				cloudformation:ResourceTypes cloudformation:RoleArn cloudformation:StackPolicyUrl cloudformation:TemplateUrl aws:RequestTag/${TagKey} aws:TagKeys	
CreateStackInstances	Grants permission to create stack instances for the specified accounts, within the specified regions	Write	stackset*		
			stackset-target		
			type		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys cloudformation:TargetRegion	
CreateStackRefactor	Grants permission to create a stack refactor	Write	stack*		
CreateStackSet	Grants permission to create a stackset as specified in the template	Write		cloudformation:RoleArn cloudformation:TemplateUrl aws:RequestTag/${TagKey} aws:TagKeys	
CreateUploadBucket [permission only]	Grants permission to upload templates to Amazon S3 buckets. Used only by the Amazon CloudFormation console and is not documented in the API reference	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeactivateOrganizationsAccess	Grants permission to deactivate trusted access between StackSets and Organizations. If trusted access is deactivated, the management account does not have permissions to create and manage service-managed StackSets for your organization	Write			
DeactivateType	Grants permission to deactivate a public extension that was previously activated in this account and region	Write			
DeleteChangeSet	Grants permission to delete the specified change set. Deleting change sets ensures that no one executes the wrong change set	Write	stack*		
				cloudformation:ChangeSetName	
DeleteGeneratedTemplate	Grants permission to delete a generated template	Write			
DeleteStack	Grants permission to delete a specified stack	Write	stack*		
				cloudformation:RoleArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteStackInstances	Grants permission to delete stack instances for the specified accounts, in the specified regions	Write	stackset*		
			stackset-target		
			type		
				cloudformation:TargetRegion	
DeleteStackSet	Grants permission to delete a specified stackset	Write	stackset*		
DeregisterType	Grants permission to deregister an existing CloudFormation type or type version	Write			
DescribeAccountLimits	Grants permission to retrieve your account's Amazon CloudFormation limits	Read			
DescribeChangeSet	Grants permission to return the description for the specified change set	Read	stack*		
				cloudformation:ChangeSetName	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeChangeSetHooks	Grants permission to return the Hook invocation information for the specified change set	Read	stack*		
				cloudformation:ChangeSetName	
DescribeGeneratedTemplate	Grants permission to describe a generated template. The output includes details about the progress of the creation of a generated template	Read			
DescribeOrganizationsAccess	Grants permission to return information about the account's OrganizationAccess status	Read			
DescribePublisher	Grants permission to return information about a CloudFormation extension publisher	Read			
DescribeResourceScan	Grants permission to describe details of a resource scan	Read			
DescribeStackDriftDetectionStatus	Grants permission to return information about a stack drift detection operation	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeStackEvents	Grants permission to return all stack related events for a specified stack	Read	stack*		
DescribeStackInstance	Grants permission to return the stack instance that's associated with the specified stack set, Amazon Web Services account, and region	Read	stackset*		
DescribeStackRefactor	Grants permission to return the description for the specified stack refactor	Read	stack*		
DescribeStackResource	Grants permission to return a description of the specified resource in the specified stack	Read	stack*		
DescribeStackResourceDrifts	Grants permission to return drift information for the resources that have been checked for drift in the specified stack	Read	stack*		
DescribeStackResources	Grants permission to return Amazon resource descriptions for running and deleted stacks	Read	stack*		
DescribeStackSet	Grants permission to return the description of the specified stack set	Read	stackset*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeStackSetOperation	Grants permission to return the description of the specified stack set operation	Read	stackset*		
DescribeStacks	Grants permission to return the description for the specified stack, and to all stacks when used in combination with the ListStacks action	List	stack		cloudformation:ListStacks
DescribeType	Grants permission to return information about the CloudFormation type requested	Read			
DescribeTypeRegistration	Grants permission to return information about the registration process for a CloudFormation type	Read			
DetectStackDrift	Grants permission to detects whether a stack's actual configuration differs, or has drifted, from it's expected configuration, as defined in the stack template and any values specified as template parameters	Read	stack*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DetectStackResourceDrift	Grants permission to return information about whether a resource's actual configuration differs, or has drifted, from it's expected configuration, as defined in the stack template and any values specified as template parameters	Read	stack*		
DetectStackSetDrift	Grants permission to enable users to detect drift on a stack set and the stack instances that belong to that stack set	Read	stackset*		
EstimateTemplateCost	Grants permission to return the estimated monthly cost of a template	Read		cloudformation:TemplateUrl	
ExecuteChangeSet	Grants permission to update a stack using the input information that was provided when the specified change set was created	Write	stack*		
				cloudformation:ChangeSetName	
ExecuteStackRefactor	Grants permission to execute a stack refactor using the input information that was provided when the specified stack refactor was created	Write	stack*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetGeneratedTemplate	Grants permission to retrieve a generated template	Read			
GetStackPolicy	Grants permission to return the stack policy for a specified stack	Read	stack*		
GetTemplate	Grants permission to return the template body for a specified stack	Read	stack*		
GetTemplateSummary	Grants permission to return information about a new or existing template	Read	stack		
			stackset		
				cloudformation:TemplateUrl	
ImportStacksToStackSet	Grants permission to enable users to import existing stacks to a new or existing stackset	Write	stackset*		
ListChangeSets	Grants permission to return the ID and status of each active change set for a stack. For example, Amazon CloudFormation lists change sets that are in the CREATE_IN_PROGRESS or CREATE_PENDING state	List	stack*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListExports	Grants permission to list all exported output values in the account and region in which you call this action	List			
ListGeneratedTemplates	Grants permission to list your generated templates in this Region	List			
ListHookResults	Grants permission to return Hook invocations result information for the specified target	List	stack		
				cloudformation:ChangeSetName	
ListImports	Grants permission to list all stacks that are importing an exported output value	List			
ListResourceScanRelatedResources	Grants permission to list the related resources for a list of resources from a resource scan. The response indicates whether each returned resource is already managed by CloudFormation	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListResourceScanResources	Grants permission to list the resources from a resource scan. The results can be filtered by resource identifier, resource type prefix, tag key, and tag value	List			
ListResourceScans	Grants permission to list the resource scans from newest to oldest. By default it will return up to 10 resource scans	List			
ListStackInstanceResourceDrifts	Grants permission to return drift information for the resources that have been checked for drift in the specified stack instance	List	stackset*		
ListStackInstances	Grants permission to return summary information about stack instances that are associated with the specified stack set	List	stackset*		
ListStackRefactorActions	Grants permission to return the list of actions of the specified stack refactor	List	stack*		
ListStackRefactors	Grants permission to return the ID and status of each active stack refactor	List	stack*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListStackResources	Grants permission to return descriptions of all resources of the specified stack	List	stack*		
ListStackSetAutoDeploymentTargets	Grants permission to return summary information about StackSet Auto Deployment Targets	List	stackset*		
ListStackSetOperationResults	Grants permission to return summary information about the results of a stack set operation	List	stackset*		
ListStackSetOperations	Grants permission to return summary information about operations performed on a stack set	List	stackset*		
ListStackSets	Grants permission to return summary information about stack sets that are associated with the user	List			
ListStacks	Grants permission to return the summary information for stacks whose status matches the specified StackStatusFilter. In combination with the DescribeStacks action, grants permission to list descriptions for stacks	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTypeRegistrations	Grants permission to list CloudFormation type registration attempts	List			
ListTypeVersions	Grants permission to list versions of a particular CloudFormation type	List			
ListTypes	Grants permission to list available CloudFormation types	List			
PublishType	Grants permission to publish the specified extension to the CloudFormation registry as a public extension in this region	Write			
RecordHandlerProgress	Grants permission to record the handler progress	Write	stack*		
RegisterPublisher	Grants permission to register account as a publisher of public extensions in the CloudFormation registry	Write			
RegisterType	Grants permission to register a new CloudFormation type	Write			
RollbackStack	Grants permission to rollback the stack to the last stable state	Write	stack*		
				cloudformation:RoleArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SetStackPolicy	Grants permission to set a stack policy for a specified stack	Permissions management	stack*		
				cloudformation:StackPolicyUrl	
SetTypeConfiguration	Grants permission to set the configuration data for a registered CloudFormation extension, in the given account and region	Write			
SetTypeDefaultVersion	Grants permission to set which version of a CloudFormation type applies to CloudFormation operations	Write			
SignalResource	Grants permission to send a signal to the specified resource with a success or failure status	Write	stack*		
StartResourceScan	Grants permission to start a scan of the resources in this account in this Region	Write			
StopStackSetOperation	Grants permission to stop an in-progress operation on a stack set and its associated stack instances	Write	stackset*		
TagResource	Grants permission to tag cloudformation resources	Tagging	changeset		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			stack		
			stackset		
				aws:TagKeys aws:RequestTag/${TagKey} cloudformation:CreateAction	
TestType	Grants permission to test a registered extension to make sure it meets all necessary requirements for being published in the CloudFormation registry	Write			
UntagResource	Grants permission to untag cloudformation resources	Tagging	changeset		
			stack		
			stackset		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys cloudformation:CreateAction	
UpdateGeneratedTemplate	Grants permission to update a generated template. This can be used to change the name, add and remove resources, refresh resources, and change the DeletionPolicy and UpdateReplacePolicy settings	Write			
UpdateStack	Grants permission to update a stack as specified in the template	Write	stack*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				cloudformation:ResourceTypes cloudformation:RoleArn cloudformation:StackPolicyUrl cloudformation:TemplateUrl aws:RequestTag/${TagKey} aws:TagKeys	
UpdateStackInstances	Grants permission to update the parameter values for stack instances for the specified accounts, within the specified regions	Write	stackset*		
			stackset-target		
			type		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				cloudformation:TargetRegion	
UpdateStackSet	Grants permission to update a stackset as specified in the template	Write	stackset*		
			stackset-target		
			type		
				cloudformation:RoleArn cloudformation:TemplateUrl cloudformation:TargetRegion aws:RequestTag/${TagKey} aws:TagKeys	
UpdateTerminationProtection	Grants permission to update termination protection for the specified stack	Write	stack*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ValidateTemplate	Grants permission to validate a specified template	Read		cloudformation:TemplateUrl	

Resource types defined by Amazon CloudFormation

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
changeset	`arn:${Partition}:cloudformation:${Region}:${Account}:changeSet/${ChangeSetName}/${Id}`	aws:ResourceTag/${TagKey}
stack	`arn:${Partition}:cloudformation:${Region}:${Account}:stack/${StackName}/${Id}`	aws:ResourceTag/${TagKey}
stackset	`arn:${Partition}:cloudformation:${Region}:${Account}:stackset/${StackSetName}:${Id}`	aws:ResourceTag/${TagKey}
stackset-target	`arn:${Partition}:cloudformation:${Region}:${Account}:stackset-target/${StackSetTarget}`	

Resource types	ARN	Condition keys
type	`arn:${Partition}:cloudformation:${Region}:${Account}:type/resource/${Type}`	
generated template	`arn:${Partition}:cloudformation:${Region}:${Account}:generatedTemplate/${Id}`	
resourcescan	`arn:${Partition}:cloudformation:${Region}:${Account}:resourceScan/${Id}`	

Condition keys for Amazon CloudFormation

Amazon CloudFormation 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 Amazon 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

Condition keys	Description	Type
cloudformation:ChangeSetName	Filters access by an Amazon CloudFormation change set name. Use to control which change sets IAM users can execute or delete	String
cloudformation:CreateAction	Filters access by the name of a resource-mutating API action. Use to control which APIs IAM users can use to add or remove tags on a stack or stack set	String
cloudformation:ImportResourceTypes	Filters access by the template resource types, such as Amazon::EC2::Instance. Use to control which resource types IAM users can work with when they want to import a resource into a stack	String
cloudformation:ResourceTypes	Filters access by the template resource types, such as Amazon::EC2::Instance. Use to control which resource types IAM users can work with when they create or update a stack	ArrayOfString
cloudformation:RoleArn	Filters access by the ARN of an IAM service role. Use to control which service role IAM users can use to work with stacks or change sets	ARN
cloudformation:StackPolicyUrl	Filters access by an Amazon S3 stack policy URL. Use to control which stack policies IAM users can associate with a stack during a create or update stack action	String
cloudformation:TargetRegion	Filters access by stack set target region. Use to control which regions IAM users can use when they create or update stack sets	ArrayOfString
cloudformation:TemplateUrl	Filters access by an Amazon S3 template URL. Use to control which templates IAM users can use when they create or update stacks	String

Actions, resources, and condition keys for Amazon CloudFront

Amazon CloudFront (service prefix: `cloudfront`) 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 CloudFront
- Resource types defined by Amazon CloudFront
- Condition keys for Amazon CloudFront

Actions defined by Amazon CloudFront

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 Amazon. 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.

> **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 distribution	Permissions management	distribution		
AssociateAlias	Grants permission to associate an alias to a CloudFront distribution	Write	distribution*		
AssociateDistributionTenantWebACL	Grants permission to associate a distribution tenant with an Amazon WAF web ACL	Write	distribution-tenant*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateDistributionWebACL	Grants permission to associate a distribution with an Amazon WAF web ACL	Write	distribution*		
CopyDistribution	Grants permission to copy an existing distribution and create a new web distribution	Write	distribution*		cloudfront:CopyDistribution cloudfront:CreateDistribution cloudfront:GetDistribution
CreateAnycastIpList	Grants permission to create an Anycast static IP list	Write	anycast-ip-list*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCachePolicy	Grants permission to add a new cache policy to CloudFront	Write	cache-policy*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCloudFrontOriginAccessIdentity	Grants permission to create a new CloudFront origin access identity	Write	origin-access-identity*		
CreateConnectionGroup	Grants permission to create a connection group	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateContinuousDeploymentPolicy	Grants permission to add a new continuous-deployment policy to CloudFront	Write	continuous-deployment-policy*		
CreateDistribution	Grants permission to create a new web distribution	Write	distribution*		cloudfront:CreateConnectionGroup
CreateDistributionTenant	Grants permission to create a distribution tenant	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateFieldLevelEncryptionConfig	Grants permission to create a new field-level encryption configuration	Write			
CreateFieldLevelEncryptionProfile	Grants permission to create a field-level encryption profile	Write			
CreateFunction	Grants permission to create a CloudFront function	Write	function*		
CreateInvalidation	Grants permission to create a new invalidation batch request	Write	distribution*		
CreateInvalidationForDistributionTenant	Grants permission to create an invalidation for a distribution tenant	Write	distribution-tenant*		
CreateKeyGroup	Grants permission to add a new key group to CloudFront	Write			
CreateKeyValueStore	Grants permission to create a CloudFront KeyValueStore	Write	key-value-store*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateMonitoringSubscription	Grants permission to enable additional CloudWatch metrics for the specified CloudFront distribution. The additional metrics incur an additional cost	Write			
CreateOriginAccessControl	Grants permission to create a new origin access control	Write			
CreateOriginRequestPolicy	Grants permission to add a new origin request policy to CloudFront	Write	origin-request-policy*		
CreatePublicKey	Grants permission to add a new public key to CloudFront	Write			
CreateRealtimeLogConfig	Grants permission to create a real-time log configuration	Write	realtime-log-config*		
CreateResponseHeadersPolicy	Grants permission to add a new response headers policy to CloudFront	Write	response-headers-policy*		
CreateSavingsPlan [permission only]	Grants permission to create a new savings plan	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateStreamingDistribution	Grants permission to create a new RTMP distribution	Write	streaming-distribution*		
CreateStreamingDistributionWithTags	Grants permission to create a new RTMP distribution with tags	Write	streaming-distribution*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateVpcOrigin	Grants permission to create a VPC origin	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAnycastIpList	Grants permission to delete an Anycast static IP list	Write	anycast-ip-list*		
DeleteCachePolicy	Grants permission to delete a cache policy	Write	cache-policy*		
DeleteCloudFrontOriginAccessIdentity	Grants permission to delete a CloudFront origin access identity	Write	origin-access-identity*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteConnectionGroup	Grants permission to delete a connection group	Write	connection-group*		
DeleteContinuousDeploymentPolicy	Grants permission to delete a continuous-deployment policy	Write	continuous-deployment-policy*		
DeleteDistribution	Grants permission to delete a web distribution	Write	distribution*		
DeleteDistributionTenant	Grants permission to delete a distribution tenant	Write	distribution-tenant*		
DeleteFieldLevelEncryptionConfig	Grants permission to delete a field-level encryption configuration	Write	field-level-encryption-config*		
DeleteFieldLevelEncryptionProfile	Grants permission to delete a field-level encryption profile	Write	field-level-encryption-profile*		
DeleteFunction	Grants permission to delete a CloudFront function	Write	function*		
DeleteKeyGroup	Grants permission to delete a key group	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteKeyValueStore	Grants permission to delete a CloudFront KeyValueStore	Write	key-value-store*		
DeleteMonitoringSubscription	Grants permission to disable additional CloudWatch metrics for the specified CloudFront distribution	Write			
DeleteOriginAccessControl	Grants permission to delete an origin access control	Write	origin-access-control*		
DeleteOriginRequestPolicy	Grants permission to delete an origin request policy	Write	origin-request-policy*		
DeletePublicKey	Grants permission to delete a public key from CloudFront	Write			
DeleteRealtimeLogConfig	Grants permission to delete a real-time log configuration	Write	realtime-log-config*		
DeleteResponseHeadersPolicy	Grants permission to delete a response headers policy	Write	response-headers-policy*		
DeleteStreamingDistribution	Grants permission to delete an RTMP distribution	Write	streaming-distribution*		
DeleteVpcOrigin	Grants permission to delete a VPC origin	Write	vpcorigin*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeFunction	Grants permission to get a CloudFront function summary	Read	function*		
DescribeKeyValueStore	Grants permission to get a CloudFront KeyValueStore summary	Read	key-value-store*		
DisassociateDistributionTenantWebACL	Grants permission to disassociate a distribution tenant from an Amazon WAF web ACL	Write	distribution-tenant*		
DisassociateDistributionWebACL	Grants permission to disassociate a distribution from an Amazon WAF web ACL	Write	distribution*		
GetAnycastIpList	Grants permission to get an Anycast static IP list	Read	anycast-ip-list*		
GetCachePolicy	Grants permission to get the cache policy	Read	cache-policy*		
GetCachePolicyConfig	Grants permission to get the cache policy configuration	Read	cache-policy*		
GetCloudFrontOriginAccessIdentity	Grants permission to get the information about a CloudFront origin access identity	Read	origin-access-identity*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCloudFrontOriginAccessIdentityConfig	Grants permission to get the configuration information about a Cloudfront origin access identity	Read	origin-access-identity*		
GetConnectionGroup	Grants permission to get information about a connection group	Read	connection-group*		
GetConnectionGroupByRoutingEndpoint	Grants permission to get information about a connection group by the specified routing endpoint	Read	connection-group*		
GetContinuousDeploymentPolicy	Grants permission to get the continuous-deployment policy	Read	continuous-deployment-policy*		
GetContinuousDeploymentPolicyConfig	Grants permission to get the continuous-deployment policy configuration	Read	continuous-deployment-policy*		
GetDistribution	Grants permission to get the information about a web distribution	Read	distribution*		
GetDistributionConfig	Grants permission to get the configuration information about a distribution	Read	distribution*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDistributionTenant	Grants permission to get information about a distribution tenant	Read	distribution-tenant*		
GetDistributionTenantByDomain	Grants permission to get information about a distribution tenant by the associated domain	Read	distribution-tenant*		
GetFieldLevelEncryption	Grants permission to get the field-level encryption configuration information	Read	field-level-encryption-config*		
GetFieldLevelEncryptionConfig	Grants permission to get the field-level encryption configuration information	Read	field-level-encryption-config*		
GetFieldLevelEncryptionProfile	Grants permission to get the field-level encryption configuration information	Read	field-level-encryption-profile*		
GetFieldLevelEncryptionProfileConfig	Grants permission to get the field-level encryption profile configuration information	Read	field-level-encryption-profile*		
GetFunction	Grants permission to get a CloudFront function's code	Read	function*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetInvalidation	Grants permission to get the information about an invalidation	Read	distribution*		
GetInvalidationForDistributionTenant	Grants permission to get information about an invalidation for a distribution tenant	Read	distribution-tenant*		
GetKeyGroup	Grants permission to get a key group	Read			
GetKeyGroupConfig	Grants permission to get a key group configuration	Read			
GetManagedCertificateDetails	Grants permission to get details about a CloudFront managed certificate	Read	distribution-tenant*		
GetMonitoringSubscription	Grants permission to get information about whether additional CloudWatch metrics are enabled for the specified CloudFront distribution	Read			
GetOriginAccessControl	Grants permission to get the origin access control	Read	origin-access-control*		
GetOriginAccessControlConfig	Grants permission to get the origin access control configuration	Read	origin-access-control*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetOriginRequestPolicy	Grants permission to get the origin request policy	Read	origin-request-policy*		
GetOriginRequestPolicyConfig	Grants permission to get the origin request policy configuration	Read	origin-request-policy*		
GetPublicKey	Grants permission to get the public key information	Read			
GetPublicKeyConfig	Grants permission to get the public key configuration information	Read			
GetRealtimeLogConfig	Grants permission to get a real-time log configuration	Read	realtime-log-config*		
GetResponseHeadersPolicy	Grants permission to get the response headers policy	Read	response-headers-policy*		
GetResponseHeadersPolicyConfig	Grants permission to get the response headers policy configuration	Read	response-headers-policy*		
GetSavingsPlan [permission only]	Grants permission to get a savings plan	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetStreamingDistribution	Grants permission to get the information about an RTMP distribution	Read	streaming-distribution*		
GetStreamingDistributionConfig	Grants permission to get the configuration information about a streaming distribution	Read	streaming-distribution*		
GetVpcOrigin	Grants permission to get the information about a VPC origin	Read	vpcorigin*		
ListAnycastIpLists	Grants permission to list your Anycast static IP lists	List			
ListCachePolicies	Grants permission to list all cache policies that have been created in CloudFront for this account	List			
ListCloudFrontOriginAccessIdentities	Grants permission to list your CloudFront origin access identities	List			
ListConflictingAliases	Grants permission to list all aliases that conflict with the given alias in CloudFront	List	distribution*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListConnectionGroups	Grants permission to list the connection groups in your Amazon Web Services account	List			
ListContinuousDeploymentPolicies	Grants permission to list all continuous-deployment policies in the account	List			
ListDistributionTenants	Grants permission to list the distribution tenants in your Amazon Web Services account	List			
ListDistributionTenantsByCustomization	Grants permission to list the distribution tenants by the customization that you specify	List			
ListDistributions	Grants permission to list the distributions associated with your Amazon Web Services account	List			
ListDistributionsByAnycastIpListId	Grants permission to list the distributions in your account that are associated with the specified AnycastIpListId	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDistributionsByCachePolicyId	Grants permission to list distribution IDs for distributions that have a cache behavior that's associated with the specified cache policy	List			
ListDistributionsByConnectionMode	Grants permission to list the distributions by the specified connection mode	List			
ListDistributionsByKeyGroup	Grants permission to list distribution IDs for distributions that have a cache behavior that's associated with the specified key group	List			
ListDistributionsByLambdaFunction [permission only]	Grants permission to list the distributions associated a Lambda function	List			
ListDistributionsByOriginRequestPolicyId	Grants permission to list distribution IDs for distributions that have a cache behavior that's associated with the specified origin request policy	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDistributionsByRealtimeLogConfig	Grants permission to get a list of distributions that have a cache behavior that's associated with the specified real-time log configuration	List			
ListDistributionsByResponseHeadersPolicyId	Grants permission to list distribution IDs for distributions that have a cache behavior that's associated with the specified response headers policy	List			
ListDistributionsByVpcOriginId	Grants permission to list IDs for distributions associated with the specified VPC origin	List			
ListDistributionsByWebACLId	Grants permission to list the distributions associated with your Amazon Web Services account with given Amazon WAF web ACL	List			
ListDomainConflicts	Grants permission to list domain conflicts for a specified domain	List	distribution		
			distribution-tenant		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListFieldLevelEncryptionConfigs	Grants permission to list all field-level encryption configurations that have been created in CloudFront for this account	List			
ListFieldLevelEncryptionProfiles	Grants permission to list all field-level encryption profiles that have been created in CloudFront for this account	List			
ListFunctions	Grants permission to get a list of CloudFront functions	List			
ListInvalidations	Grants permission to list your invalidation batches	List	distribution*		
ListInvalidationsForDistributionTenant	Grants permission to list the invalidations for a distribution tenant	List	distribution-tenant*		
ListKeyGroups	Grants permission to list all key groups that have been created in CloudFront for this account	List			
ListKeyValueStores	Grants permission to get a list of CloudFront KeyValueStores	List			
ListOriginAccessControls	Grants permission to list all origin access controls in the account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListOriginRequestPolicies	Grants permission to list all origin request policies that have been created in CloudFront for this account	List			
ListPublicKeys	Grants permission to list all public keys that have been added to CloudFront for this account	List			
ListRateCards [permission only]	Grants permission to list CloudFront rate cards for the account	List			
ListRealtimeLogConfigs	Grants permission to get a list of real-time log configurations	List			
ListResponseHeadersPolicies	Grants permission to list all response headers policies that have been created in CloudFront for this account	List			
ListSavingsPlans [permission only]	Grants permission to list savings plans in the account	List			
ListStreamingDistributions	Grants permission to list your RTMP distributions	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to list tags for a CloudFront resource	Read	anycast-ip-list		
			connection-group		
			distribution		
			distribution-tenant		
			vpcorigin		
ListUsages [permission only]	Grants permission to list CloudFront usage	List			
ListVpcOrigins	Grants permission to list VPC origins	List			
PublishFunction	Grants permission to publish a CloudFront function	Write	function*		
TagResource	Grants permission to add tags to a CloudFront resource	Tagging	anycast-ip-list		
			connection-group		
			distribution		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			distribution-tenant		
			streaming-distribution		
			vpcorigin		
				aws:RequestTag/${TagKey} aws:TagKeys	
TestFunction	Grants permission to test a CloudFront function	Write	function*		
UntagResource	Grants permission to remove tags from a CloudFront resource	Tagging	anycast-ip-list		
			connection-group		
			distribution		
			distribution-tenant		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			streaming-distribution		
			vpcorigin		
				aws:TagKeys	
UpdateCachePolicy	Grants permission to update a cache policy	Write	cache-policy*		
UpdateCloudFrontOriginAccessIdentity	Grants permission to set the configuration for a CloudFront origin access identity	Write	origin-access-identity*		
UpdateConnectionGroup	Grants permission to update a connection group	Write	connection-group*		
UpdateContinuousDeploymentPolicy	Grants permission to update a continuous-deployment policy	Write	continuous-deployment-policy*		
UpdateDistribution	Grants permission to update the configuration for a web distribution	Write	distribution*		
UpdateDistributionTenant	Grants permission to update a distribution tenant	Write	distribution-tenant*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateDistributionWithStagingConfig	Grants permission to copy the configuration from a staging web distribution to its corresponding primary web distribution	Write	distribution*		
UpdateDomainAssociation	Grants permission to update a domain association	Write	distribution		
			distribution-tenant		
UpdateFieldLevelEncryptionConfig	Grants permission to update a field-level encryption configuration	Write			
UpdateFieldLevelEncryptionProfile	Grants permission to update a field-level encryption profile	Write	field-level-encryption-profile*		
UpdateFunction	Grants permission to update a CloudFront function	Write	function*		
UpdateKeyGroup	Grants permission to update a key group	Write			
UpdateKeyValueStore	Grants permission to update a CloudFront KeyValueStore	Write	key-value-store*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateOriginAccessControl	Grants permission to update an origin access control	Write	origin-access-control*		
UpdateOriginRequestPolicy	Grants permission to update an origin request policy	Write	origin-request-policy*		
UpdatePublicKey	Grants permission to update public key information	Write			
UpdateRealtimeLogConfig	Grants permission to update a real-time log configuration	Write	realtime-log-config*		
UpdateResponseHeadersPolicy	Grants permission to update a response headers policy	Write	response-headers-policy*		
UpdateSavingsPlan [permission only]	Grants permission to update a savings plan	Write			
UpdateStreamingDistribution	Grants permission to update the configuration for an RTMP distribution	Write	streaming-distribution*		
UpdateVpcOrigin	Grants permission to update a VPC origin	Write	vpcorigin*		
VerifyDnsConfiguration	Grants permission to verify the DNS configuration for a specified domain	Read	distribution-tenant		

Resource types defined by Amazon CloudFront

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
distribution	`arn:${Partition}:cloudfront::${Account}:distribution/${DistributionId}`	aws:ResourceTag/${TagKey}
streaming-distribution	`arn:${Partition}:cloudfront::${Account}:streaming-distribution/${DistributionId}`	aws:ResourceTag/${TagKey}
origin-access-identity	`arn:${Partition}:cloudfront::${Account}:origin-access-identity/${Id}`	
field-level-encryption-config	`arn:${Partition}:cloudfront::${Account}:field-level-encryption-config/${Id}`	
field-level-encryption-profile	`arn:${Partition}:cloudfront::${Account}:field-level-encryption-profile/${Id}`	
cache-policy	`arn:${Partition}:cloudfront::${Account}:cache-policy/${Id}`	
origin-request-policy	`arn:${Partition}:cloudfront::${Account}:origin-request-policy/${Id}`	
realtime-log-config	`arn:${Partition}:cloudfront::${Account}:realtime-log-config/${Name}`	

Resource types	ARN	Condition keys
function	arn:${Partition}:cloudfront::${Account}:function/${Name}	
key-value-store	arn:${Partition}:cloudfront::${Account}:key-value-store/${Name}	
response-headers-policy	arn:${Partition}:cloudfront::${Account}:response-headers-policy/${Id}	
origin-access-control	arn:${Partition}:cloudfront::${Account}:origin-access-control/${Id}	
continuous-deployment-policy	arn:${Partition}:cloudfront::${Account}:continuous-deployment-policy/${Id}	
anycast-ip-list	arn:${Partition}:cloudfront::${Account}:anycast-ip-list/${Id}	aws:ResourceTag/${TagKey}
vpcorigin	arn:${Partition}:cloudfront::${Account}:vpcorigin/${Id}	aws:ResourceTag/${TagKey}
distribution-tenant	arn:${Partition}:cloudfront::${Account}:distribution-tenant/${Id}	aws:ResourceTag/${TagKey}
connection-group	arn:${Partition}:cloudfront::${Account}:connection-group/${Id}	aws:ResourceTag/${TagKey}

Condition keys for Amazon CloudFront

Amazon CloudFront 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 Amazon 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 CloudTrail

Amazon 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 Amazon CloudTrail
- Resource types defined by Amazon CloudTrail
- Condition keys for Amazon CloudTrail

Actions defined by Amazon 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 Amazon. 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.

> **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/${TagKey} aws:TagKeys	
CancelQuery	Grants permission to cancel a running query	Write	eventdatastore*		
CreateChannel	Grants permission to create a channel	Write	channel*		cloudtrail:AddTags
			eventdatastore*		
				aws:RequestTag/${TagKey} aws:TagKeys	

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateServiceLinkedChannel [permission only]	Grants permission to create a service-linked channel that specifies the settings for delivery of log data to an Amazon 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
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteChannel	Grants permission to delete a channel	Write	channel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
DeregisterOrganizationDelegatedAdmin	Grants permission to deregister an Amazon Organizations member account as a delegated administrator	Write			organizations:DeregisterDelegatedAdministrator organizations:ListAWSServiceAccessForOrganization

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
DisableFederation	Grants permission to disable federation of event data store data by using the Amazon 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 Amazon 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*		
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 Amazon Glue Data Catalog	Read	eventdatastore*		kms:Decrypt kms:GenerateDataKey
GetEventSelectors	Grants permission to list settings for event selectors configured for a trail	Read	trail*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
GetTrail	Grants permission to list settings for the trail	Read	trail*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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
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			
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 Amazon 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 Amazon 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 Amazon 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 Amazon 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 Amazon 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 Amazon CloudTrail works with IAM in the *Amazon 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 Amazon CloudTrail

Amazon 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 Amazon 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 Amazon. 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.

> **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*		
CreateServiceLevelObjective	Grants permission to create a service level objective	Write		aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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*		
DescribeAlarms	Grants permission to describe all alarms, currently owned by the user's account	Read	alarm*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
EnableTopologyDiscovery	Grants permission to enable a CloudWatch topology discovery	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GenerateQuery	Grants permission to generate a Metrics Insights or Logs Insights query string from a natural language prompt	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			
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*		

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 Amazon Web Services account owner	List			
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 insight-rule		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			slo		
	SCENARIO: CloudWatch-Alarm		alarm*		
	SCENARIO: CloudWatch-InsightRule		insight-rule*		
	SCENARIO: CloudWatch-ServiceLevelObjective		slo*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutInsightRule	Grants permission to create a new insight rule or replace an existing insight rule	Write	insight-rule*		
				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		
			insight-rule		
			slo		
				aws:TagKeys aws:RequestTag/${TagKey}	
	SCENARIO: CloudWatch-Alarm		alarm*		
	SCENARIO: CloudWatch-InsightRule		insight-rule*		
	SCENARIO: CloudWatch-ServiceLevelObjective		slo*		
UntagResource	Grants permission to remove a tag from an Amazon CloudWatch resource	Tagging	alarm		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			insight-rule		
			slo		
				aws:TagKeys	
	SCENARIO: CloudWatch-Alarm		alarm*		
	SCENARIO: CloudWatch-InsightRule		insight-rule*		
	SCENARIO: CloudWatch-ServiceLevelObjective		slo*		
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/${TagKey}
service	arn:${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 Amazon 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:requestInsightRuleLogGroups	Filters actions based on the Log Groups specified in an Insight Rule	ArrayOfString
cloudwatch:requestManagedResourceARNs	Filters access by the Resource ARNs specified in a managed Insight Rule	ArrayOfARN

Actions, resources, and condition keys for Amazon CloudWatch Application Insights

Amazon CloudWatch Application Insights (service prefix: `applicationinsights`) 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 Application Insights
- Resource types defined by Amazon CloudWatch Application Insights
- Condition keys for Amazon CloudWatch Application Insights

Actions defined by Amazon CloudWatch Application 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 Amazon. 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.

> **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
AddWorkload	Grants permission to add a workload	Write			
CreateApplication	Grants permission to create an application from a resource group	Write			
CreateComponent	Grants permission to create a component from a group of resources	Write			
CreateLogPattern	Grants permission to create log a pattern	Write			
DeleteApplication	Grants permission to delete an application	Write			
DeleteComponent	Grants permission to delete a component	Write			
DeleteLogPattern	Grants permission to delete a log pattern	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeApplication	Grants permission to describe an application	Read			
DescribeComponent	Grants permission to describe a component	Read			
DescribeComponentConfiguration	Grants permission to describe a component's configuration	Read			
DescribeComponentConfigurationRecommendation	Grants permission to describe the recommended application component configuration	Read			
DescribeLogPattern	Grants permission to describe a log pattern	Read			
DescribeObservation	Grants permission to describe an observation	Read			
DescribeProblem	Grants permission to describe a problem	Read			
DescribeProblemObservations	Grants permission to describe the observation in a problem	Read			
DescribeWorkload	Grants permission to describe a workload	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Link [permission only]	Grants permission to share Application Insights resources with a monitoring account	Write			
ListApplications	Grants permission to list all applications	List			
ListComponents	Grants permission to list an application's components	List			
ListConfigurationHistory	Grants permission to list configuration history	List			
ListLogPatternSets	Grants permission to list log pattern sets for an application	List			
ListLogPatterns	Grants permission to list log patterns	List			
ListProblems	Grants permission to list the problems in an application	List			
ListTagsForResource	Grants permission to list tags for the resource	Read			
ListWorkloads	Grants permission to list workloads	List			
RemoveWorkload	Grants permission to remove a workload	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to tag a resource	Tagging		aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a resource	Tagging		aws:TagKeys	
UpdateApplication	Grants permission to update an application	Write			
UpdateComponent	Grants permission to update a component	Write			
UpdateComponentConfiguration	Grants permission to update a component's configuration	Write			
UpdateLogPattern	Grants permission to update a log pattern	Write			
UpdateProblem	Grants permission to update a problem	Write			
UpdateWorkload	Grants permission to update a workload	Write			

Resource types defined by Amazon CloudWatch Application Insights

Amazon CloudWatch Application Insights does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon CloudWatch Application Insights, specify `"Resource": "*"` in your policy.

Condition keys for Amazon CloudWatch Application Insights

Amazon CloudWatch Application 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 Amazon 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

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 Amazon. 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.

> **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 Amazon Key Management Service (Amazon KMS) customer master key (CMK) with the specified log group	Write	log-group*		
CancelExportTask	Grants permission to cancel an export task if it is in PENDING or RUNNING state	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/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
CreateLogAnomalyDetector	Grants permission to create a log anomaly detector	Write	log-group*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateLogDelivery [permission only]	Grants permission to create the log delivery	Write			
CreateLogGroup	Grants permission to create a new log group with the specified name	Write	log-group*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLogStream	Grants permission to create a new log stream with the specified name	Write	log-stream*		
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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		
DeleteQueryDefinition	Grants permission to delete a saved CloudWatch Logs Insights query definition	Write			

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDeliverySources	Grants permission to retrieve a list of delivery sources in an account	List			
DescribeDestinations	Grants permission to return all the destinations that are associated with the Amazon Web Services account making the request	List			
DescribeExportTasks	Grants permission to return all the export tasks that are associated with the Amazon Web Services account making the request	List			
DescribeFieldIndexes	Grants permission to return all the indexing attributes that are attached with the log groups	List			
DescribeIndexPolicies	Grants permission to return all the index policies that are attached with the log groups	List			
DescribeLogGroups	Grants permission to return all the log groups that are associated with the Amazon Web Services account making the request	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
DescribeSubscriptionFilters	Grants permission to return all the subscription filters associated with the specified log group	List	log-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateKmsKey	Grants permission to disassociate the associated Amazon Key Management Service (Amazon KMS) customer master key (CMK) from the specified log group	Write	log-group*		
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*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		
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*		
GetTransformer	Grants permission to return transformer associated with the specified log group	Read	log-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Link [permission only]	Grants permission to share CloudWatch resources with a monitoring account	Write			
ListAnomalies	Grants permission to list all anomalies detected in the Amazon Web Services 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 Amazon Web Services account making the request	List			
ListLogAnomalyDetectors	Grants permission to return all the anomaly detectors that are associated with the Amazon Web Services 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
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			
ListTagsForResource	Grants permission to list the tags for the specified resource	List	anomaly-detector		
			delivery		
			delivery-destination		
			delivery-source		
			destination		
			log-group		
ListTagsLogGroup	Grants permission to list the tags for the specified log group	List	log-group*		
PutAccountPolicy	Grants permission to attach an account policy	Write			

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey} logs:LogGeneratingResourceArns	
PutDestination	Grants permission to create or update a Destination	Write	destination*		iam:PassRole
				aws:TagKeys aws:RequestTag/${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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
PutMetricFilter	Grants permission to create or update a metric filter and associates it with the specified log group	Write	log-group*		
PutQueryDefinition	Grants permission to create or update a query definition	Write			
PutResourcePolicy	Grants permission to create or update a resource policy allowing other Amazon 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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutTransformer	Grants permission to create or update a transformer and associates it with the specified log group	Write	log-group*		
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}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to add or update the specified tags for the specified resource	Tagging	anomaly-detector		
			delivery		
			delivery-destination		
			delivery-source		
			destination		
			log-group		
				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		
				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			

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}

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 Amazon 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:LogGenerating ResourceArns	Filters access by the Log Generating Resource ARNs passed in the request	ArrayOfARN

Actions, resources, and condition keys for Amazon CloudWatch Observability Access Manager

Amazon CloudWatch Observability Access Manager (service prefix: `oam`) 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 Observability Access Manager
- Resource types defined by Amazon CloudWatch Observability Access Manager
- Condition keys for Amazon CloudWatch Observability Access Manager

Actions defined by Amazon CloudWatch Observability Access 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 Amazon. 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.

> **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
CreateLink	Grants permission to create a link between a monitoring account and a source account for cross-account monitoring	Write	Sink*		oam:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys oam:ResourceTypes	
CreateSink	Grants permission to create a sink in an account so that it can be used as a monitoring account for cross-account monitoring	Write		aws:RequestTag/${TagKey} aws:TagKeys	oam:TagResource
DeleteLink	Grants permission to delete a link between a monitoring	Write	Link*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	account and a source account for cross-account monitoring			aws:ResourceTag/${TagKey}	
DeleteSink	Grants permission to delete a cross-account monitoring sink in a monitoring account	Write	Sink*		
				aws:ResourceTag/${TagKey}	
GetLink	Grants permission to retrieve complete information about one cross-account monitoring link	Read	Link*		
				aws:ResourceTag/${TagKey}	
GetSink	Grants permission to retrieve complete information about one cross-account monitoring sink	Read	Sink*		
				aws:ResourceTag/${TagKey}	
GetSinkPolicy	Grants permission to retrieve information for the IAM policy for a cross-account monitoring sink	Read	Sink*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAttachedLinks	Grants permission to retrieve a list of links that are linked for a cross-account monitoring sink	Read	Sink*		
				aws:ResourceTag/${TagKey}	
ListLinks	Grants permission to retrieve the ARNs of cross-account monitoring links in this account	Read			
ListSinks	Grants permission to retrieve the ARNs of cross-account monitoring sinks in this account	Read			
ListTagsForResource	Grants permission to list the tags for a resource	Read	Link		
			Sink		
PutSinkPolicy	Grants permission to create or update the IAM policy for a cross-account monitoring sink	Write	Sink*		
				aws:ResourceTag/${TagKey}	
TagResource	Grants permission to tag a resource	Tagging	Link		
			Sink		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a resource	Tagging	Link		
			Sink		
				aws:TagKeys	
UpdateLink	Grants permission to update an existing link between a monitoring account and a source account	Write	Link*		
				aws:ResourceTag/${TagKey} oam:ResourceTypes	

Resource types defined by Amazon CloudWatch Observability Access 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
Link	`arn:${Partition}:oam:${Region}:${Account}:link/${ResourceId}`	aws:ResourceTag/${TagKey}
Sink	`arn:${Partition}:oam:${Region}:${Account}:sink/${ResourceId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon CloudWatch Observability Access Manager

Amazon CloudWatch Observability Access 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 Amazon 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
oam:ResourceTypes	Filters access by the presence of resource types in the request	ArrayOfString

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 Amazon. 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.

> **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/${TagKey} aws:TagKeys	
CreateCanary	Grants permission to create a canary	Write		aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
DescribeCanaries	Grants permission to list information of all canaries	Read		synthetics:Names	

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
ListGroupResources	Grants permission to list information about canaries in a group	List	group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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	
StartCaneryDryRun	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	

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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/${TagKey}
group	`arn:${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 Amazon 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 Amazon CodeBuild

Amazon CodeBuild (service prefix: `codebuild`) 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 CodeBuild
- Resource types defined by Amazon CodeBuild
- Condition keys for Amazon CodeBuild

Actions defined by Amazon CodeBuild

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 Amazon. 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.

> **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
BatchDeleteBuilds	Grants permission to delete one or more builds	Write	project*		
BatchGetBuildBatches	Grants permission to get information about one or more build batches	Read	project*		
BatchGetBuilds	Grants permission to get information about one or more builds	Read	project*		
BatchGetCommandExecutions	Grants permission to get information about one or more command executions	Read	sandbox*		
BatchGetFleets	Grants permission to return an array of the Fleet objects specified by the input parameter	Read	fleet*		
BatchGetProjects	Grants permission to get information about one or more build projects	Read	project*		
BatchGetReportGroups	Grants permission to return an array of ReportGroup objects that are specified by the input reportGroupArns parameter	Read	report-group*		
BatchGetReports	Grants permission to return an array of the Report	Read	report-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	objects specified by the input reportArns parameter				
BatchGetSandboxes	Grants permission to get information about one or more sandboxes	Read	project*		
BatchPutCodeCoverages [permission only]	Grants permission to add or update information about a report	Write	report-group*		
BatchPutTestCases [permission only]	Grants permission to add or update information about a report	Write	report-group*		
CreateFleet	Grants permission to create a compute fleet	Write	fleet*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys codebuild:imageId codebuild:computeType codebuild:vpcConfig codebuild:vpcConfig.vpcId codebuild:vpcConfig.securityGroupIds codebuild:vpcConfig.subnets codebuild:computeC	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				onfiguration codebuild:computeConfiguration.disk codebuild:computeConfiguration.instanceType codebuild:computeConfiguration.machineType codebuild:computeConfiguration.memory codebuild:computeConfiguration.vCpu codebuild:environmentType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:fleetServiceRole	
CreateProject	Grants permission to create a build project	Write	project*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys codebuild:autoRetryLimit codebuild:concurrentBuildLimit codebuild:artifacts codebuild:artifacts.bucketOwnerAccess codebuild:artifacts.encryptionDisabled codebuild:artifact	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s.location codebuild:secondaryArtifacts codebuild:secondaryArtifacts.artifactIdentifier codebuild:secondaryArtifacts.bucketOwnerAccess codebuild:secondaryArtifacts.encryptionDisabled codebuild:secondaryArtifact	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s.location codebuild:secondaryArtifacts/${artifactIdentifier}.bucketOwnerAccess codebuild:secondaryArtifacts/${artifactIdentifier}.encryptionDisabled codebuild:secondaryArtifacts/${artifactIdentifier}.location codebuild:source	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:source.buildStatusConfig.targetUrl codebuild:source.buildStatusConfig.context codebuild:source.location codebuild:source.insecureSsl codebuild:source.buildspec codebuild:source.auth.resource codebuild:source.auth.type	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:secondarySources codebuild:secondarySources.sourceIdentifier codebuild:secondarySources.buildStatusConfig.targetUrl codebuild:secondarySources.buildStatusConfig.context codebuild:secondarySources.location codebuild:secondarySources.	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				auth.resource codebuild:secondarySources.auth.type codebuild:secondarySources.buildspec codebuild:secondarySources.insecureSsl codebuild:secondarySources/${sourceIdentifier}.buildStatusConfig.targetUrl codebuild:secondarySources/${sourceI	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				dentifier}.buildStatusConfig.context codebuild:secondarySources/${sourceIdentifier}.location codebuild:secondarySources/${sourceIdentifier}.auth.resource codebuild:secondarySources/${sourceIdentifier}.auth.type codebuild:secondarySources/${sourceIdentifier	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				}.buildspec codebuild:secondarySources/${sourceIdentifier}.insecureSsl codebuild:logsConfig codebuild:logsConfig.s3Logs codebuild:logsConfig.s3Logs.bucketOwnerAccess codebuild:logsConfig.s3Logs.encryptionDisabled codebuild:logsConf	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ig.s3Logs.location codebuild:logsConfig.s3Logs.status codebuild:fileSystemLocations.identifier codebuild:fileSystemLocations.type codebuild:fileSystemLocations.location codebuild:fileSystemLocations/${identifier}.type	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:fileSystemLocations/${identifier}.location codebuild:buildBatchConfig codebuild:buildBatchConfig.serviceRole codebuild:buildBatchConfig.restrictions.computeTypesAllowed codebuild:buildBatchConfig.restrictions.fleetsAllowed	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:vpcConfig codebuild:vpcConfig.subnets codebuild:vpcConfig.vpcId codebuild:vpcConfig.securityGroupIds codebuild:environment codebuild:environment.type codebuild:environment.fleet.fleetArn codebuild:environment.computeType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:environment.image codebuild:environment.imagePullCredentialsType codebuild:environment.privilegedMode codebuild:environment.certificate codebuild:environment.computeConfiguration codebuild:environment.computeConfiguration.disk	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:environment.computeConfiguration.instanceType codebuild:environment.computeConfiguration.machineType codebuild:environment.computeConfiguration.memory codebuild:environment.computeConfiguration.vCpu codebuild:environment.envir	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				onmentVariables codebuild:environment.environmentVariables.name codebuild:environment.environmentVariables.value codebuild:environment.environmentVariables/${name}.value codebuild:environment.registryCredential codebuild:environm	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ent.registryCredential.credential codebuild:environment.registryCredential.credentialProvider codebuild:encryptionKey codebuild:cache codebuild:cache.type codebuild:cache.location codebuild:cache.modes	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:serviceRole	
CreateReport [permission only]	Grants permission to create a report. A report is created when tests specified in the buildspec file for a report groups run during the build of a project	Write	report-group*		
CreateReportGroup	Grants permission to create a report group	Write	report-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys codebuild:exportConfig.s3Destination.bucket codebuild:exportConfig.s3Destination.bucketOwner codebuild:exportConfig.s3Destination.encryptionKey codebuild:exportConfig.s3Destination.encrypti	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				onDisabled codebuild:exportConfig.s3Destination.path	
CreateWebhook	Grants permission to create webhook. For an existing Amazon CodeBuild build project that has its source code stored in a GitHub or Bitbucket repository, enables Amazon CodeBuild to start rebuilding the source code every time a code change is pushed to the repository	Write	project*		
				codebuild:buildType codebuild:manualCreation codebuild:scopeConfiguration.domain codebuild:scopeConfiguration.name codebuild:scopeConfiguration.scope	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteBuildBatch	Grants permission to delete a build batch	Write	project*		
DeleteFleet	Grants permission to delete a compute fleet	Write	fleet*		
DeleteOAuthToken [permission only]	Grants permission to delete an OAuth token from a connected third-party OAuth provider. Only used in the Amazon CodeBuild console	Write			
DeleteProject	Grants permission to delete a build project	Write	project*		
DeleteReport	Grants permission to delete a report	Write	report-group*		
DeleteReportGroup	Grants permission to delete a report group	Write	report-group*		
DeleteResourcePolicy	Grants permission to delete a resource policy for the associated project or report group	Permissions management	project		
			report-group		
DeleteSourceCredentials	Grants permission to delete a set of GitHub, GitHub Enterprise, or Bitbucket source credentials	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteWebhook	Grants permission to delete webhook. For an existing Amazon CodeBuild build project that has its source code stored in a GitHub or Bitbucket repository, stops Amazon CodeBuild from rebuilding the source code every time a code change is pushed to the repository	Write	project*		
DescribeCodeCoverages	Grants permission to return an array of CodeCoverage objects	Read	report-group*		
DescribeTestCases	Grants permission to return an array of TestCase objects	Read	report-group*		
GetReportGroupTrend	Grants permission to analyze and accumulate test report values for the test reports in the specified report group	Read	report-group*		
GetResourcePolicy	Grants permission to return a resource policy for the specified project or report group	Read	project		
			report-group		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportSourceCredentials	Grants permission to import the source repository credentials for an Amazon CodeBuild project that has its source code stored in a GitHub, GitHub Enterprise, or Bitbucket repository	Write		codebuild:authType codebuild:serverType codebuild:shouldOverwrite codebuild:token codebuild:username	
InvalidateProjectCache	Grants permission to reset the cache for a project	Write	project*		
ListBuildBatches	Grants permission to get a list of build batch IDs, with each build batch ID representing a single build batch	List			
ListBuildBatchesForProject	Grants permission to get a list of build batch IDs for the specified build project, with each build batch ID representing a single build batch	List	project*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListBuilds	Grants permission to get a list of build IDs, with each build ID representing a single build	List			
ListBuildsForProject	Grants permission to get a list of build IDs for the specified build project, with each build ID representing a single build	List	project*		
ListCommandExecutionsForSandbox	Grants permission to get a list of command execution IDs for the specified sandbox, with each command execution ID representing a single command execution	List	sandbox*		
ListConnectedOAuthAccounts [permission only]	Grants permission to list connected third-party OAuth providers. Only used in the Amazon CodeBuild console	List			
ListCuratedEnvironmentImages	Grants permission to get information about Docker images that are managed by Amazon CodeBuild	List			
ListFleets	Grants permission to get a list of compute fleet ARNs, with each compute fleet ARN representing a single fleet	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListProjects	Grants permission to get a list of build project names, with each build project name representing a single build project	List			
ListReportGroups	Grants permission to return a list of report group ARNs. Each report group ARN represents one report group	List			
ListReports	Grants permission to return a list of report ARNs. Each report ARN representing one report	List			
ListReportsForReportGroup	Grants permission to return a list of report ARNs that belong to the specified report group. Each report ARN represents one report	List	report-group*		
ListRepositories [permission only]	Grants permission to list source code repositories from a connected third-party OAuth provider. Only used in the Amazon CodeBuild console	List			
ListSandboxes	Grants permission to get a list of sandbox IDs, with each sandbox ID representing a single sandbox	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListSandboxesForProject	Grants permission to get a list of sandbox IDs for the specified sandbox project, with each sandbox ID representing a single sandbox	List	project*		
ListSharedProjects	Grants permission to return a list of project ARNs that have been shared with the requester. Each project ARN represents one project	List			
ListSharedReportGroups	Grants permission to return a list of report group ARNs that have been shared with the requester. Each report group ARN represents one report group	List			
ListSourceCredentials	Grants permission to return a list of SourceCredentialsInfo objects	List			
PersistOAuthToken [permission only]	Grants permission to save an OAuth token from a connected third-party OAuth provider. Only used in the Amazon CodeBuild console	Write			
PutResourcePolicy	Grants permission to create a resource policy for the associated project or report group	Permissions management	project		
			report-group		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RetryBuild	Grants permission to retry a build	Write	project*		
RetryBuildBatch	Grants permission to retry a build batch	Write	project*		
StartBuild	Grants permission to start running a build	Write	project*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:autoRetryLimit codebuild:artifacts codebuild:artifacts.bucketOwnerAccess codebuild:artifacts.encryptionDisabled codebuild:artifacts.location codebuild:secondaryArtifacts codebuild:secondaryArtifacts.artifac	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tIdentifier codebuild:secondaryArtifacts.bucketOwnerAccess codebuild:secondaryArtifacts.encryptionDisabled codebuild:secondaryArtifacts.location codebuild:secondaryArtifacts/${artifactIdentifier}.bucketOwnerAccess	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:secondaryArtifacts/${artifactIdentifier}.encryptionDisabled codebuild:secondaryArtifacts/${artifactIdentifier}.location codebuild:source codebuild:source.buildStatusConfig.targetUrl codebuild:source.buildStatusConfig.context	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:source.location codebuild:source.insecureSsl codebuild:source.buildspec codebuild:source.auth.resource codebuild:source.auth.type codebuild:secondarySources codebuild:secondarySources.sourceIdentifier codebuild:secondar	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ySources.buildStatusConfig.targetUrl codebuild:secondarySources.buildStatusConfig.context codebuild:secondarySources.location codebuild:secondarySources.auth.resource codebuild:secondarySources.auth.type codebuild:secondarySources.buildspec	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:secondarySources.insecureSsl codebuild:secondarySources/${sourceIdentifier}.buildStatusConfig.targetUrl codebuild:secondarySources/${sourceIdentifier}.buildStatusConfig.context codebuild:secondarySources/${sourceIdentifier}.location	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:secondarySources/${sourceIdentifier}.auth.resource codebuild:secondarySources/${sourceIdentifier}.auth.type codebuild:secondarySources/${sourceIdentifier}.buildspec codebuild:secondarySources/${sourceIdentifier}.insecureSsl	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:logsConfig codebuild:logsConfig.s3Logs codebuild:logsConfig.s3Logs.bucketOwnerAccess codebuild:logsConfig.s3Logs.encryptionDisabled codebuild:logsConfig.s3Logs.location codebuild:logsConfig.s3Logs.status codebuild:environment	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:environment.type codebuild:environment.fleet.fleetArn codebuild:environment.computeType codebuild:environment.image codebuild:environment.imagePullCredentialsType codebuild:environment.privilegedMode codebuild:environment.certificate	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:environment.environmentVariables codebuild:environment.environmentVariables.name codebuild:environment.environmentVariables.value codebuild:environment.environmentVariables/${name}.value codebuild:environment.registryCredential	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:environment.registryCredential.credential codebuild:environment.registryCredential.credentialProvider codebuild:encryptionKey codebuild:cache codebuild:cache.type codebuild:cache.location codebuild:cache.modes	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:serviceRole	
StartBuildBatch	Grants permission to start running a build batch	Write	project*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:artifacts codebuild:artifacts.bucketOwnerAccess codebuild:artifacts.encryptionDisabled codebuild:artifacts.location codebuild:secondaryArtifacts codebuild:secondaryArtifacts.artifactIdentifier	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:secondaryArtifacts.bucketOwnerAccess codebuild:secondaryArtifacts.encryptionDisabled codebuild:secondaryArtifacts.location codebuild:secondaryArtifacts/${artifactIdentifier}.bucketOwnerAccess codebuild:secondaryArtifacts/${artif	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				actIdentifier}.encryptionDisabled codebuild:secondaryArtifacts/${artifactIdentifier}.location codebuild:source codebuild:source.location codebuild:source.insecureSsl codebuild:source.buildspec codebuild:source.auth.resource	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:source.auth.type codebuild:secondarySources codebuild:secondarySources.sourceIdentifier codebuild:secondarySources.buildStatusConfig.targetUrl codebuild:secondarySources.buildStatusConfig.context codebuild:secondarySources.location	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:secondarySources.auth.resource codebuild:secondarySources.auth.type codebuild:secondarySources.buildspec codebuild:secondarySources.insecureSsl codebuild:secondarySources/${sourceIdentifier}.buildStatusConfig.targetUrl	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:secondarySources/${sourceIdentifier}.buildStatusConfig.context codebuild:secondarySources/${sourceIdentifier}.location codebuild:secondarySources/${sourceIdentifier}.auth.resource codebuild:secondarySources/${sourceIdentifier}.auth.type	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:secondarySources/${sourceIdentifier}.buildspec codebuild:secondarySources/${sourceIdentifier}.insecureSsl codebuild:logsConfig codebuild:logsConfig.s3Logs codebuild:logsConfig.s3Logs.bucketOwnerAccess codebuild:logsConfig.s3Logs	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				.encryptionDisabled codebuild:logsConfig.s3Logs.location codebuild:logsConfig.s3Logs.status codebuild:buildBatchConfig codebuild:buildBatchConfig.serviceRole codebuild:buildBatchConfig.restrictions.computeTypesAllowed codebuild:buildBat	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				chConfig.restrictions.fleetsAllowed codebuild:environment codebuild:environment.type codebuild:environment.computeType codebuild:environment.image codebuild:environment.imagePullCredentialsType codebuild:environment.privilegedMode	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:environment.certificate codebuild:environment.environmentVariables codebuild:environment.environmentVariables.name codebuild:environment.environmentVariables.value codebuild:environment.environmentVariables/${name}.value	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:environment.registryCredential codebuild:environment.registryCredential.credential codebuild:environment.registryCredential.credentialProvider codebuild:encryptionKey codebuild:cache codebuild:cache.type	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:cache.location codebuild:cache.modes codebuild:serviceRole	
StartCommandExecution	Grants permission to start running a command execution	Write	sandbox*		
StartSandbox	Grants permission to start running a sandbox	Write	project*		
StartSandboxConnection	Grants permission to establish a connection to the sandbox	Write	sandbox*		
StopBuild	Grants permission to attempt to stop running a build	Write	project*		
StopBuildBatch	Grants permission to attempt to stop running a build batch	Write	project*		
StopSandbox	Grants permission to attempt to stop running a sandbox	Write	project*		
UpdateFleet	Grants permission to change the settings of an existing compute fleet	Write	fleet*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys codebuild:imageId codebuild:computeType codebuild:vpcConfig codebuild:vpcConfig.vpcId codebuild:vpcConfig.securityGroupIds codebuild:vpcConfig.subnets codebuild:computeC	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				onfiguration codebuild:computeConfiguration.disk codebuild:computeConfiguration.instanceType codebuild:computeConfiguration.machineType codebuild:computeConfiguration.memory codebuild:computeConfiguration.vCpu codebuild:environmentType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:fleetServiceRole	
UpdateProject	Grants permission to change the settings of an existing build project	Write	project*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys codebuild:autoRetryLimit codebuild:concurrentBuildLimit codebuild:artifacts codebuild:artifacts.bucketOwnerAccess codebuild:artifacts.encryptionDisabled codebuild:artifact	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s.location codebuild:secondaryArtifacts codebuild:secondaryArtifacts.artifactIdentifier codebuild:secondaryArtifacts.bucketOwnerAccess codebuild:secondaryArtifacts.encryptionDisabled codebuild:secondaryArtifact	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s.location codebuild:secondaryArtifacts/${artifactIdentifier}.bucketOwnerAccess codebuild:secondaryArtifacts/${artifactIdentifier}.encryptionDisabled codebuild:secondaryArtifacts/${artifactIdentifier}.location codebuild:source	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:source.buildStatusConfig.targetUrl codebuild:source.buildStatusConfig.context codebuild:source.location codebuild:source.insecureSsl codebuild:source.buildspec codebuild:source.auth.resource codebuild:source.auth.type	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:secondarySources codebuild:secondarySources.sourceIdentifier codebuild:secondarySources.buildStatusConfig.targetUrl codebuild:secondarySources.buildStatusConfig.context codebuild:secondarySources.location codebuild:secondarySources.	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				auth.resource codebuild:secondarySources.auth.type codebuild:secondarySources.buildspec codebuild:secondarySources.insecureSsl codebuild:secondarySources/${sourceIdentifier}.buildStatusConfig.targetUrl codebuild:secondarySources/${sourceI	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				dentifier}.buildStatusConfig.context codebuild:secondarySources/${sourceIdentifier}.location codebuild:secondarySources/${sourceIdentifier}.auth.resource codebuild:secondarySources/${sourceIdentifier}.auth.type codebuild:secondarySources/${sourceIdentifier	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				}.buildspec codebuild:secondarySources/${sourceIdentifier}.insecureSsl codebuild:logsConfig codebuild:logsConfig.s3Logs codebuild:logsConfig.s3Logs.bucketOwnerAccess codebuild:logsConfig.s3Logs.encryptionDisabled codebuild:logsConf	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ig.s3Logs.location codebuild:logsConfig.s3Logs.status codebuild:fileSystemLocations.identifier codebuild:fileSystemLocations.type codebuild:fileSystemLocations.location codebuild:fileSystemLocations/${identifier}.type	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:fileSystemLocations/${identifier}.location codebuild:buildBatchConfig codebuild:buildBatchConfig.serviceRole codebuild:buildBatchConfig.restrictions.computeTypesAllowed codebuild:buildBatchConfig.restrictions.fleetsAllowed	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:vpcConfig codebuild:vpcConfig.subnets codebuild:vpcConfig.vpcId codebuild:vpcConfig.securityGroupIds codebuild:environment codebuild:environment.type codebuild:environment.fleet.fleetArn codebuild:environment.computeType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:environment.image codebuild:environment.imagePullCredentialsType codebuild:environment.privilegedMode codebuild:environment.certificate codebuild:environment.computeConfiguration codebuild:environment.computeConfiguration.disk	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:environment.computeConfiguration.instanceType codebuild:environment.computeConfiguration.machineType codebuild:environment.computeConfiguration.memory codebuild:environment.computeConfiguration.vCpu codebuild:environment.envir	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				onmentVariables codebuild:environment.environmentVariables.name codebuild:environment.environmentVariables.value codebuild:environment.environmentVariables/${name}.value codebuild:environment.registryCredential codebuild:environm	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ent.registryCredential.credential codebuild:environment.registryCredential.credentialProvider codebuild:encryptionKey codebuild:cache codebuild:cache.type codebuild:cache.location codebuild:cache.modes	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				codebuild:serviceRole	
UpdateProjectVisibility	Grants permission to change the public visibility of a project and its builds	Write	project*		
				aws:RequestTag/${TagKey} aws:TagKeys codebuild:projectVisibility	
UpdateReport [permission only]	Grants permission to update information about a report	Write	report-group*		
UpdateReportGroup	Grants permission to change the settings of an existing report group	Write	report-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys codebuild:exportConfig.s3Destination.bucket codebuild:exportConfig.s3Destination.bucketOwner codebuild:exportConfig.s3Destination.encryptionKey codebuild:exportConfig.s3Destination.encrypti	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				onDisabled codebuild:exportConfig.s3Destination.path	
UpdateWebhook	Grants permission to update the webhook associated with an Amazon CodeBuild build project	Write	project*		
				codebuild:buildType codebuild:manualCreation codebuild:scopeConfiguration.domain codebuild:scopeConfiguration.name codebuild:scopeConfiguration.scope	

Resource types defined by Amazon CodeBuild

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
build	`arn:${Partition}:codebuild:${Region}:${Account}:build/${BuildId}`	
build-batch	`arn:${Partition}:codebuild:${Region}:${Account}:build-batch/${BuildBatchId}`	
project	`arn:${Partition}:codebuild:${Region}:${Account}:project/${ProjectName}`	aws:ResourceTag/${TagKey}
report-group	`arn:${Partition}:codebuild:${Region}:${Account}:report-group/${ReportGroupName}`	aws:ResourceTag/${TagKey}
report	`arn:${Partition}:codebuild:${Region}:${Account}:report/${ReportGroupName}:${ReportId}`	
fleet	`arn:${Partition}:codebuild:${Region}:${Account}:fleet/${FleetName}:${FleetId}`	
sandbox	`arn:${Partition}:codebuild:${Region}:${Account}:sandbox/${SandboxId}`	

Condition keys for Amazon CodeBuild

Amazon CodeBuild 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 Amazon 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
aws:TagKeys	Filters access by actions based on the presence of tag keys in the request	ArrayOfString
codebuild:artifacts	Filters access by the API corresponding argument value	Bool
codebuild:artifacts.bucketOwnerAccess	Filters access by the API corresponding argument value	String
codebuild:artifacts.encryptionDisabled	Filters access by the API corresponding argument value	Bool
codebuild:artifacts.location	Filters access by the API corresponding argument value	String

Condition keys	Description	Type
codebuild:authType	Filters access by the API corresponding argument value	String
codebuild:autoRetryLimit	Filters access by the API corresponding argument value	Numeric
codebuild:buildArn	Filters access by the ARN of the Amazon CodeBuild build from which the request originated	ARN
codebuild:buildBatchConfig	Filters access by the API corresponding argument value	Bool
codebuild:buildBatchConfig.restrictions.computeTypesAllowed	Filters access by the API corresponding argument value	ArrayOfString
codebuild:buildBatchConfig.restrictions.fleetsAllowed	Filters access by the API corresponding argument value	ArrayOfString
codebuild:buildBatchConfig.serviceRole	Filters access by the API corresponding argument value	String
codebuild:buildType	Filters access by the API corresponding argument value	String
codebuild:cache	Filters access by the API corresponding argument value	Bool

Condition keys	Description	Type
codebuild:cache.location	Filters access by the API corresponding argument value	String
codebuild:cache.modes	Filters access by the API corresponding argument value	ArrayOfString
codebuild:cache.type	Filters access by the API corresponding argument value	String
codebuild:computeConfiguration	Filters access by the API corresponding argument value	Bool
codebuild:computeConfiguration.disk	Filters access by the API corresponding argument value	Numeric
codebuild:computeConfiguration.instanceType	Filters access by the API corresponding argument value	String
codebuild:computeConfiguration.machineType	Filters access by the API corresponding argument value	String
codebuild:computeConfiguration.memory	Filters access by the API corresponding argument value	Numeric
codebuild:computeConfiguration.vCpu	Filters access by the API corresponding argument value	Numeric

Condition keys	Description	Type
codebuild:computeType	Filters access by the API corresponding argument value	String
codebuild:concurrentBuildLimit	Filters access by the API corresponding argument value	Numeric
codebuild:encryptionKey	Filters access by the API corresponding argument value	String
codebuild:environment	Filters access by the API corresponding argument value	Bool
codebuild:environment.certificate	Filters access by the API corresponding argument value	String
codebuild:environment.computeConfiguration	Filters access by the API corresponding argument value	Bool
codebuild:environment.computeConfiguration.disk	Filters access by the API corresponding argument value	Numeric
codebuild:environment.computeConfiguration.instanceType	Filters access by the API corresponding argument value	String

Condition keys	Description	Type
codebuild:environment.computeConfiguration.machineType	Filters access by the API corresponding argument value	String
codebuild:environment.computeConfiguration.memory	Filters access by the API corresponding argument value	Numeric
codebuild:environment.computeConfiguration.vCpu	Filters access by the API corresponding argument value	Numeric
codebuild:environment.computeType	Filters access by the API corresponding argument value	String
codebuild:environment.environmentVariables	Filters access by the API corresponding argument value	Bool
codebuild:environment.environmentVariables.name	Filters access by the API corresponding argument value	ArrayOfString

Condition keys	Description	Type
codebuild:environment.environmentVariables.value	Filters access by the API corresponding argument value	ArrayOfString
codebuild:environment.environmentVariables/${name}.value	Filters access by the API corresponding argument value	String
codebuild:environment.fleet.fleetArn	Filters access by the API corresponding argument value	ARN
codebuild:environment.image	Filters access by the API corresponding argument value	String
codebuild:environment.imagePullCredentialsType	Filters access by the API corresponding argument value	String
codebuild:environment.privilegedMode	Filters access by the API corresponding argument value	Bool

Condition keys	Description	Type
codebuild:environment.registryCredential	Filters access by the API corresponding argument value	Bool
codebuild:environment.registryCredential.credential	Filters access by the API corresponding argument value	String
codebuild:environment.registryCredential.credentialProvider	Filters access by the API corresponding argument value	String
codebuild:environment.type	Filters access by the API corresponding argument value	String
codebuild:environmentType	Filters access by the API corresponding argument value	String
codebuild:exportConfig.s3Destination.bucket	Filters access by the API corresponding argument value	String
codebuild:exportConfig.s3Destination.bucketOwner	Filters access by the API corresponding argument value	String

Condition keys	Description	Type
codebuild:exportConfig.s3Destination.encryptionDisabled	Filters access by the API corresponding argument value	Bool
codebuild:exportConfig.s3Destination.encryptionKey	Filters access by the API corresponding argument value	String
codebuild:exportConfig.s3Destination.path	Filters access by the API corresponding argument value	String
codebuild:fileSystemLocations.identifier	Filters access by the API corresponding argument value	ArrayOfString
codebuild:fileSystemLocations.location	Filters access by the API corresponding argument value	ArrayOfString
codebuild:fileSystemLocations.type	Filters access by the API corresponding argument value	ArrayOfString

Condition keys	Description	Type
codebuild:fileSystemLocations/${identifier}.location	Filters access by the API corresponding argument value	String
codebuild:fileSystemLocations/${identifier}.type	Filters access by the API corresponding argument value	String
codebuild:fleetServiceRole	Filters access by the API corresponding argument value	String
codebuild:imageId	Filters access by the API corresponding argument value	String
codebuild:logsConfig	Filters access by the API corresponding argument value	Bool
codebuild:logsConfig.s3Logs	Filters access by the API corresponding argument value	Bool
codebuild:logsConfig.s3Logs.bucketOwnerAccess	Filters access by the API corresponding argument value	String
codebuild:logsConfig.s3Logs.encryptionDisabled	Filters access by the API corresponding argument value	Bool

Condition keys	Description	Type
codebuild:logsConfig.s3Logs.location	Filters access by the API corresponding argument value	String
codebuild:logsConfig.s3Logs.status	Filters access by the API corresponding argument value	String
codebuild:manualCreation	Filters access by the API corresponding argument value	Bool
codebuild:projectArn	Filters access by the ARN of the Amazon CodeBuild project from which the request originated	ARN
codebuild:projectVisibility	Filters access by the API corresponding argument value	String
codebuild:scopeConfiguration.domain	Filters access by the API corresponding argument value	String
codebuild:scopeConfiguration.name	Filters access by the API corresponding argument value	String
codebuild:scopeConfiguration.scope	Filters access by the API corresponding argument value	String
codebuild:secondaryArtifacts	Filters access by the API corresponding argument value	Bool

Condition keys	Description	Type
codebuild:secondaryArtifacts.artifactIdentifier	Filters access by the API corresponding argument value	ArrayOfString
codebuild:secondaryArtifacts.bucketOwnerAccess	Filters access by the API corresponding argument value	ArrayOfString
codebuild:secondaryArtifacts.encryptionDisabled	Filters access by the API corresponding argument value	ArrayOfBool
codebuild:secondaryArtifacts.location	Filters access by the API corresponding argument value	ArrayOfString
codebuild:secondaryArtifacts/${artifactIdentifier}.bucketOwnerAccess	Filters access by the API corresponding argument value	String
codebuild:secondaryArtifacts/${artifactIdentifier}.encryptionDisabled	Filters access by the API corresponding argument value	Bool

Condition keys	Description	Type
codebuild:secondaryArtifacts/${artifactIdentifier}.location	Filters access by the API corresponding argument value	String
codebuild:secondarySources	Filters access by the API corresponding argument value	Bool
codebuild:secondarySources.auth.resource	Filters access by the API corresponding argument value	ArrayOfString
codebuild:secondarySources.auth.type	Filters access by the API corresponding argument value	ArrayOfString
codebuild:secondarySources.buildStatusConfig.context	Filters access by the API corresponding argument value	ArrayOfString
codebuild:secondarySources.buildStatusConfig.targetUrl	Filters access by the API corresponding argument value	ArrayOfString

Condition keys	Description	Type
codebuild:secondarySources.buildspec	Filters access by the API corresponding argument value	Bool
codebuild:secondarySources.insecureSsl	Filters access by the API corresponding argument value	ArrayOfBool
codebuild:secondarySources.location	Filters access by the API corresponding argument value	ArrayOfString
codebuild:secondarySources.sourceIdentifier	Filters access by the API corresponding argument value	ArrayOfString
codebuild:secondarySources/${sourceIdentifier}.auth.resource	Filters access by the API corresponding argument value	String
codebuild:secondarySources/${sourceIdentifier}.auth.type	Filters access by the API corresponding argument value	String

Condition keys	Description	Type
codebuild:secondarySources/${sourceIdentifier}.buildStatusConfig.context	Filters access by the API corresponding argument value	String
codebuild:secondarySources/${sourceIdentifier}.buildStatusConfig.targetUrl	Filters access by the API corresponding argument value	String
codebuild:secondarySources/${sourceIdentifier}.buildspec	Filters access by the API corresponding argument value	Bool
codebuild:secondarySources/${sourceIdentifier}.insecureSsl	Filters access by the API corresponding argument value	Bool

Condition keys	Description	Type
codebuild:secondarySources/${sourceIdentifier}.location	Filters access by the API corresponding argument value	String
codebuild:serverType	Filters access by the API corresponding argument value	String
codebuild:serviceRole	Filters access by the API corresponding argument value	String
codebuild:shouldOverwrite	Filters access by the API corresponding argument value	Bool
codebuild:source	Filters access by the API corresponding argument value	Bool
codebuild:source.auth.resource	Filters access by the API corresponding argument value	String
codebuild:source.auth.type	Filters access by the API corresponding argument value	String
codebuild:source.buildStatusConfig.context	Filters access by the API corresponding argument value	String

Condition keys	Description	Type
codebuild:source.buildStatusConfig.targetUrl	Filters access by the API corresponding argument value	String
codebuild:source.buildspec	Filters access by the API corresponding argument value	Bool
codebuild:source.insecureSsl	Filters access by the API corresponding argument value	Bool
codebuild:source.location	Filters access by the API corresponding argument value	String
codebuild:token	Filters access by the API corresponding argument value	String
codebuild:username	Filters access by the API corresponding argument value	String
codebuild:vpcConfig	Filters access by the API corresponding argument value	Bool
codebuild:vpcConfig.securityGroupIds	Filters access by the API corresponding argument value	ArrayOfString
codebuild:vpcConfig.subnets	Filters access by the API corresponding argument value	ArrayOfString
codebuild:vpcConfig.vpcId	Filters access by the API corresponding argument value	String

Actions, resources, and condition keys for Amazon CodeCommit

Amazon CodeCommit (service prefix: `codecommit`) 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 CodeCommit
- Resource types defined by Amazon CodeCommit
- Condition keys for Amazon CodeCommit

Actions defined by Amazon CodeCommit

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 Amazon. 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.

> **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
AssociateApprovalRuleTemplateWithRepository	Grants permission to associate an approval rule template with a repository	Write	repository*		
BatchAssociateApprovalRuleTemplateWithRepositories	Grants permission to associate an approval rule template with multiple repositories in a single operation	Write	repository*		
BatchDescribeMergeConflicts	Grants permission to get information about multiple merge conflicts when	Read	repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	attempting to merge two commits using either the three-way merge or the squash merge option				
BatchDisassociateApprovalRuleTemplateFromRepositories	Grants permission to remove the association between an approval rule template and multiple repositories in a single operation	Write	repository*		
BatchGetCommits	Grants permission to return information about one or more commits in an Amazon CodeCommit repository	Read	repository*		
BatchGetPullRequests [permission only]	Grants permission to return information about one or more pull requests in an Amazon CodeCommit repository	Read	repository*		
BatchGetRepositories	Grants permission to get information about multiple repositories	Read	repository*		
CancelUploadArchive [permission only]	Grants permission to cancel the uploading of an archive to a pipeline in Amazon CodePipeline	Read	repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateApprovalRuleTemplate	Grants permission to create an approval rule template that will automatically create approval rules in pull requests that match the conditions defined in the template; does not grant permission to create approval rules for individual pull requests	Write			
CreateBranch	Grants permission to create a branch in an Amazon CodeCommit repository with this API; does not control Git create branch actions	Write	repository*		
				codecommit:References	
CreateCommit	Grants permission to add, copy, move or update single or multiple files in a branch in an Amazon CodeCommit repository, and generate a commit for the changes in the specified branch	Write	repository*		
				codecommit:References	
CreatePullRequest	Grants permission to create a pull request in the specified repository	Write	repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePullRequestApprovalRule	Grants permission to create an approval rule specific to an individual pull request; does not grant permission to create approval rule templates	Write	repository*		
CreateRepository	Grants permission to create an Amazon CodeCommit repository	Write	repository*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUnreferencedMergeCommit	Grants permission to create an unreferenced commit that contains the result of merging two commits using either the three-way or the squash merge option; does not control Git merge actions	Write	repository*		
				codecommit:References	
DeleteApprovalRuleTemplate	Grants permission to delete an approval rule template	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteBranch	Grants permission to delete a branch in an Amazon CodeCommit repository with this API; does not control Git delete branch actions	Write	repository*		
				codecommit:References	
DeleteCommentContent	Grants permission to delete the content of a comment made on a change, file, or commit in a repository	Write	repository*		
DeleteFile	Grants permission to delete a specified file from a specified branch	Write	repository*		
				codecommit:References	
DeletePullRequestApprovalRule	Grants permission to delete approval rule created for a pull request if the rule was not created by an approval rule template	Write	repository*		
DeleteRepository	Grants permission to delete an Amazon CodeCommit repository	Write	repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeMergeConflicts	Grants permission to get information about specific merge conflicts when attempting to merge two commits using either the three-way or the squash merge option	Read	repository*		
DescribePullRequestEvents	Grants permission to return information about one or more pull request events	Read	repository*		
DisassociateApprovalRuleTemplateFromRepository	Grants permission to remove the association between an approval rule template and a repository	Write	repository*		
EvaluatePullRequestApprovalRules	Grants permission to evaluate whether a pull request is mergable based on its current approval state and approval rule requirements	Read	repository*		
GetApprovalRuleTemplate	Grants permission to return information about an approval rule template	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetBlob	Grants permission to view the encoded content of an individual file in an Amazon CodeCommit repository from the Amazon CodeCommit console	Read	repository*		
GetBranch	Grants permission to get details about a branch in an Amazon CodeCommit repository with this API; does not control Git branch actions	Read	repository*		
GetComment	Grants permission to get the content of a comment made on a change, file, or commit in a repository	Read	repository*		
GetCommentReactions	Grants permission to get the reactions on a comment	Read	repository*		
GetCommentsForComparedCommit	Grants permission to get information about comments made on the comparison between two commits	Read	repository*		
GetCommentsForPullRequest	Grants permission to get comments made on a pull request	Read	repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCommit	Grants permission to return information about a commit, including commit message and committer information, with this API; does not control Git log actions	Read	repository*		
GetCommitHistory [permission only]	Grants permission to get information about the history of commits in a repository	Read	repository*		
GetCommitsFromMergeBase [permission only]	Grants permission to get information about the difference between commits in the context of a potential merge	Read	repository*		
GetDifferences	Grants permission to view information about the differences between valid commit specifiers such as a branch, tag, HEAD, commit ID, or other fully qualified reference	Read	repository*		
GetFile	Grants permission to return the base-64 encoded contents of a specified file and its metadata	Read	repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetFolder	Grants permission to return the contents of a specified folder in a repository	Read	repository*		
GetMergeCommit	Grants permission to get information about a merge commit created by one of the merge options for pull requests that creates merge commits. Not all merge options create merge commits. This permission does not control Git merge actions	Read	repository*		
				codecommit:References	
GetMergeConflicts	Grants permission to get information about merge conflicts between the before and after commit IDs for a pull request in a repository	Read	repository*		
GetMergeOptions	Grants permission to get information about merge options for pull requests that can be used to merge two commits; does not control Git merge actions	Read	repository*		
GetObjectIdentifier [permission only]	Grants permission to resolve blobs, trees, and commits to their identifier	Read	repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetPullRequest	Grants permission to get information about a pull request in a specified repository	Read	repository*		
GetPullRequestApprovalStates	Grants permission to retrieve the current approvals on an inputted pull request	Read	repository*		
GetPullRequestOverrideState	Grants permission to retrieve the current override state of a given pull request	Read	repository*		
GetReferences [permission only]	Grants permission to get details about references in an Amazon CodeCommit repository; does not control Git reference actions	Read	repository*		
GetRepository	Grants permission to get information about an Amazon CodeCommit repository	Read	repository*		
GetRepositoryTriggers	Grants permission to get information about triggers configured for a repository	Read	repository*		
GetTree [permission only]	Grants permission to view the contents of a specified tree in an Amazon CodeCommit repository from the Amazon CodeCommit console	Read	repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetUploadArchiveStatus [permission only]	Grants permission to get status information about an archive upload to a pipeline in Amazon CodePipeline	Read	repository*		
GitPull [permission only]	Grants permission to pull information from an Amazon CodeCommit repository to a local repo	Read	repository*		
GitPush [permission only]	Grants permission to push information from a local repo to an Amazon CodeCommit repository	Write	repository*		
				codecommit:References	
ListApprovalRuleTemplates	Grants permission to list all approval rule templates in an Amazon Web Services Region for the Amazon Web Services account	List			
ListAssociatedApprovalRuleTemplatesForRepository	Grants permission to list approval rule templates that are associated with a repository	List	repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListBranches	Grants permission to list branches for an Amazon CodeCommit repository with this API; does not control Git branch actions	List	repository*		
ListFileCommitHistory	Grants permission to list commits and changes to a specified file	List	repository*		
ListPullRequests	Grants permission to list pull requests for a specified repository	List	repository*		
ListRepositories	Grants permission to list information about Amazon CodeCommit repositories in the current Region for your Amazon Web Services account	List			
ListRepositoriesForApprovalRuleTemplate	Grants permission to list repositories that are associated with an approval rule template	List			
ListTagsForResource	Grants permission to list the resource attached to a CodeCommit resource ARN	List	repository		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
MergeBranchesByFastForward	Grants permission to merge two commits into the specified destination branch using the fast-forward merge option	Write	repository*		
				codecommit:References	
MergeBranchesBySquash	Grants permission to merge two commits into the specified destination branch using the squash merge option	Write	repository*		
				codecommit:References	
MergeBranchesByThreeWay	Grants permission to merge two commits into the specified destination branch using the three-way merge option	Write	repository*		
				codecommit:References	
MergePullRequestByFastForward	Grants permission to close a pull request and attempt to merge it into the specified destination branch for that pull request at the specified commit using the fast-forward merge option	Write	repository*		
				codecommit:References	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
MergePullRequestBySquash	Grants permission to close a pull request and attempt to merge it into the specified destination branch for that pull request at the specified commit using the squash merge option	Write	repository*		
				codecommit:References	
MergePullRequestByThreeWay	Grants permission to close a pull request and attempt to merge it into the specified destination branch for that pull request at the specified commit using the three-way merge option	Write	repository*		
				codecommit:References	
OverridePullRequestApprovalRules	Grants permission to override all approval rules for a pull request, including approval rules created by a template	Write	repository*		
PostCommentForComparedCommit	Grants permission to post a comment on the comparison between two commits	Write	repository*		
PostCommentForPullRequest	Grants permission to post a comment on a pull request	Write	repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PostCommentReply	Grants permission to post a comment in reply to a comment on a comparison between commits or a pull request	Write	repository*		
PutCommentReaction	Grants permission to post a reaction on a comment	Write	repository*		
PutFile	Grants permission to add or update a file in a branch in an Amazon CodeCommit repository, and generate a commit for the addition in the specified branch	Write	repository*		
				codecommit:References	
PutRepositoryTriggers	Grants permission to create, update, or delete triggers for a repository	Write	repository*		
TagResource	Grants permission to attach resource tags to a CodeCommit resource ARN	Tagging	repository		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
TestRepositoryTriggers	Grants permission to test the functionality of repository triggers by sending information to the trigger target	Write	repository*		
UntagResource	Grants permission to disassociate resource tags from a CodeCommit resource ARN	Tagging	repository		
				aws:TagKeys aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateApprovalRuleTemplateContent	Grants permission to update the content of approval rule templates; does not grant permission to update content of approval rules created specifically for pull requests	Write			
UpdateApprovalRuleTemplateDescription	Grants permission to update the description of approval rule templates	Write			
UpdateApprovalRuleTemplateName	Grants permission to update the name of approval rule templates	Write			
UpdateComment	Grants permission to update the contents of a comment if the identity matches the identity used to create the comment	Write	repository*		
UpdateDefaultBranch	Grants permission to change the default branch in an Amazon CodeCommit repository	Write	repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdatePullRequestApprovalRuleContent	Grants permission to update the content for approval rules created for a specific pull requests; does not grant permission to update approval rule content for rules created with an approval rule template	Write	repository*		
UpdatePullRequestApprovalState	Grants permission to update the approval state for pull requests	Write	repository*		
UpdatePullRequestDescription	Grants permission to update the description of a pull request	Write	repository*		
UpdatePullRequestStatus	Grants permission to update the status of a pull request	Write	repository*		
UpdatePullRequestTitle	Grants permission to update the title of a pull request	Write	repository*		
UpdateRepositoryDescription	Grants permission to change the description of an Amazon CodeCommit repository	Write	repository*		
UpdateRepositoryEncryptionKey	Grants permission to change the Amazon KMS encryption key used to encrypt and decrypt an Amazon CodeCommit repository	Write	repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateRepositoryName	Grants permission to change the name of an Amazon CodeCommit repository	Write	repository*		
UploadArchive [permission only]	Grants permission to the service role for Amazon CodePipeline to upload repository changes into a pipeline	Write	repository*		

Resource types defined by Amazon CodeCommit

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:${Partition}:codecommit:${Region}:${Account}:${RepositoryName}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon CodeCommit

Amazon CodeCommit 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 Amazon 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
codecommit:References	Filters access by Git reference to specified Amazon CodeCommit actions	String

Actions, resources, and condition keys for Amazon CodeDeploy

Amazon CodeDeploy (service prefix: `codedeploy`) 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 CodeDeploy
- Resource types defined by Amazon CodeDeploy
- Condition keys for Amazon CodeDeploy

Actions defined by Amazon CodeDeploy

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 Amazon. 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.

> **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
AddTagsToOnPremisesInstances	Grants permission to add tags to one or more on-premises instances	Tagging	instance*		
BatchGetApplicationRevisions	Grants permission to get information about one or more application revisions	Read	application*		
BatchGetApplications	Grants permission to get information about multiple applications associated with the IAM user	Read	application*		
BatchGetDeploymentGroups	Grants permission to get information about one or more deployment groups	Read	deploymentgroup*		
BatchGetDeploymentInstances	Grants permission to get information about one or more instance that are part of a deployment group	Read	deploymentgroup*		
BatchGetDeploymentTargets	Grants permission to return an array of one or more targets associated with a deployment. This method works with all compute types and should be used instead of the deprecated BatchGetDeploymentInstances. The maximum number of targets that can be returned is 25	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetDeployments	Grants permission to get information about multiple deployments associated with the IAM user	Read	deploymentgroup*		
BatchGetOnPremisesInstances	Grants permission to get information about one or more on-premises instances	Read	instance*		
ContinueDeployment	Grants permission to start the process of rerouting traffic from instances in the original environment to instances in thereplacement environment without waiting for a specified wait time to elapse	Write			
CreateApplication	Grants permission to create an application associated with the IAM user	Write	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCloudFormationDeployment [permission only]	Grants permission to create CloudFormation deployment to cooperate ochestration for a CloudFormation stack update	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDeployment	Grants permission to create a deployment for an application associated with the IAM user	Write	deploymentgroup*		
CreateDeploymentConfig	Grants permission to create a custom deployment configuration associated with the IAM user	Write	deploymentconfig*		
CreateDeploymentGroup	Grants permission to create a deployment group for an application associated with the IAM user	Write	deploymentgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteApplication	Grants permission to delete an application associated with the IAM user	Write	application*		
DeleteDeploymentConfig	Grants permission to delete a custom deployment configuration associated with the IAM user	Write	deploymentconfig*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteDeploymentGroup	Grants permission to delete a deployment group for an application associated with the IAM user	Write	deploymentgroup*		
DeleteGitHubAccountToken	Grants permission to delete a GitHub account connection	Write			
DeleteResourcesByExternalId	Grants permission to delete resources associated with the given external Id	Write			
DeregisterOnPremisesInstance	Grants permission to deregister an on-premises instance	Write	instance*		
GetApplication	Grants permission to get information about a single application associated with the IAM user	List	application*		
GetApplicationRevision	Grants permission to get information about a single application revision for an application associated with the IAM user	List	application*		
GetDeployment	Grants permission to get information about a single deployment to a deployment group for an application associated with the IAM user	List	deploymentgroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDeploymentConfig	Grants permission to get information about a single deployment configuration associated with the IAM user	List	deploymentconfig*		
GetDeploymentGroup	Grants permission to get information about a single deployment group for an application associated with the IAM user	List	deploymentgroup*		
GetDeploymentInstance	Grants permission to get information about a single instance in a deployment associated with the IAM user	List	deploymentgroup*		
GetDeploymentTarget	Grants permission to return information about a deployment target	Read			
GetOnPremisesInstance	Grants permission to get information about a single on-premises instance	List	instance*		
ListApplicationRevisions	Grants permission to get information about all application revisions for an application associated with the IAM user	List	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListApplications	Grants permission to get information about all applications associated with the IAM user	List			
ListDeploymentConfigs	Grants permission to get information about all deployment configurations associated with the IAM user	List			
ListDeploymentGroups	Grants permission to get information about all deployment groups for an application associated with the IAM user	List	application*		
ListDeploymentInstances	Grants permission to get information about all instances in a deployment associated with the IAM user	List	deploymentgroup*		
ListDeploymentTargets	Grants permission to return an array of target IDs that are associated a deployment	List			
ListDeployments	Grants permission to get information about all deployments to a deployment group associated with the IAM user, or to get all deployments associated with the IAM user	List	deploymentgroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListGitHubAccountTokenNames	Grants permission to list the names of stored connections to GitHub accounts	List			
ListOnPremisesInstances	Grants permission to get a list of one or more on-premises instance names	List			
ListTagsForResource	Grants permission to return a list of tags for the resource identified by a specified ARN. Tags are used to organize and categorize your CodeDeploy resources	List	application		
			deploymentgroup		
PutLifecycleEventHookExecutionStatus	Grants permission to notify a lifecycle event hook execution status for associated deployment with the IAM user	Write			
RegisterApplicationRevision	Grants permission to register information about an application revision for an application associated with the IAM user	Write	application*		
RegisterOnPremisesInstance	Grants permission to register an on-premises instance	Write	instance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RemoveTagsFromOnPremisesInstances	Grants permission to remove tags from one or more on-premises instances	Tagging	instance*		
SkipWaitTimeForInstanceTermination	Grants permission to override any specified wait time and starts terminating instances immediately after the traffic routing is complete. This action applies to blue-green deployments only	Write			
StopDeployment	Grants permission to stop a deployment	Write			
TagResource	Grants permission to associate the list of tags in the input Tags parameter with the resource identified by the ResourceArn input parameter	Tagging	application		
			deploymentgroup		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagResource	Grants permission to disassociate a resource from a list of tags. The resource is identified by the ResourceArn input parameter. The tags are identfied by the list of keys in the TagKeys input parameter	Tagging	application		
			deploymentgroup		
				aws:TagKeys	
UpdateApplication	Grants permission to update an application	Write	application*		
UpdateDeploymentGroup	Grants permission to change information about a single deployment group for an application associated with the IAM user	Write	deploymentgroup*		

Resource types defined by Amazon CodeDeploy

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:${Partition}:codedeploy:${Region}:${Account}:application:${ApplicationName}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
deploymentconfig	`arn:${Partition}:codedeploy:${Region}:${Account}:deploymentconfig:${DeploymentConfigurationName}`	
deploymentgroup	`arn:${Partition}:codedeploy:${Region}:${Account}:deploymentgroup:${ApplicationName}/${DeploymentGroupName}`	aws:ResourceTag/${TagKey}
instance	`arn:${Partition}:codedeploy:${Region}:${Account}:instance:${InstanceName}`	

Condition keys for Amazon CodeDeploy

Amazon CodeDeploy 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 Amazon global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters actions based on the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters actions based on tag key-value pairs attached to the resource	String
aws:TagKeys	Filters actions based on the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for Amazon CodeDeploy secure host commands service

Amazon CodeDeploy secure host commands service (service prefix: `codedeploy-commands-secure`) 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 CodeDeploy secure host commands service
- Resource types defined by Amazon CodeDeploy secure host commands service
- Condition keys for Amazon CodeDeploy secure host commands service

Actions defined by Amazon CodeDeploy secure host commands 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 Amazon. 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.

> **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
GetDeploymentSpecification	Grants permission to get deployment specification	Read			
PollHostCommand	Grants permission to request host agent commands	Read			
PutHostCommandAcknowledgement	Grants permission to mark host agent commands acknowledged	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutHostCommandComplete	Grants permission to mark host agent commands completed	Write			

Resource types defined by Amazon CodeDeploy secure host commands service

Amazon CodeDeploy secure host commands service does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon CodeDeploy secure host commands service, specify `"Resource": "*"` in your policy.

Condition keys for Amazon CodeDeploy secure host commands service

CodeDeploy Commands Secure 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 Amazon global condition context keys.

Actions, resources, and condition keys for Amazon CodePipeline

Amazon CodePipeline (service prefix: `codepipeline`) 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 CodePipeline
- Resource types defined by Amazon CodePipeline
- Condition keys for Amazon CodePipeline

Actions defined by Amazon CodePipeline

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 Amazon. 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.

> **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
AcknowledgeJob	Grants permission to view information about a specified job and whether that job has been received by the job worker	Write			
AcknowledgeThirdPartyJob	Grants permission to confirm that a job worker has received the specified job (partner actions only)	Write			
CreateCustomActionType	Grants permission to create a custom action that you can use in the pipelines associated with your Amazon Web Services account	Write	actiontype*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePipeline	Grants permission to create a uniquely named pipeline	Write	pipeline*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteCustomActionType	Grants permission to delete a custom action	Write	actiontype*		
DeletePipeline	Grants permission to delete a specified pipeline	Write	pipeline*		
DeleteWebhook	Grants permission to delete a specified webhook	Write	webhook*		
DeregisterWebhookWithThirdParty	Grants permission to remove the registration of a webhook with the third party specified in its configuration	Write	webhook*		
DisableStageTransition	Grants permission to prevent revisions from transitioning to the next stage in a pipeline	Write	stage*		
EnableStageTransition	Grants permission to allow revisions to transition to the next stage in a pipeline	Write	stage*		
GetActionType	Grants permission to view information about an action type	Read			
GetJobDetails	Grants permission to view information about a job (custom actions only)	Read			
GetPipeline	Grants permission to retrieve information about a pipeline structure	Read	pipeline*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetPipelineExecution	Grants permission to view information about an execution of a pipeline, including details about artifacts, the pipeline execution ID, and the name, version, and status of the pipeline	Read	pipeline*		
GetPipelineState	Grants permission to view information about the current state of the stages and actions of a pipeline	Read	pipeline*		
GetThirdPartyJobDetails	Grants permission to view the details of a job for a third-party action (partner actions only)	Read			
ListActionExecutions	Grants permission to list the action executions that have occurred in a pipeline	Read	pipeline*		
ListActionTypes	Grants permission to list a summary of all the action types available for pipelines in your account	Read			
ListDeployActionExecutionTargets	Grants permission to list the deployment details for deploy action executions that have occurred in a pipeline	Read	pipeline*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPipelineExecutions	Grants permission to list a summary of the most recent executions for a pipeline	List	pipeline*		
ListPipelines	Grants permission to list a summary of all the pipelines associated with your Amazon Web Services account	List			
ListRuleExecutions	Grants permission to list the rule executions that have occurred in a pipeline	Read	pipeline*		
ListRuleTypes	Grants permission to list a summary of all the rule types available for pipelines in your account	Read			
ListTagsForResource	Grants permission to list tags for a CodePipeline resource	Read	actiontype		
			pipeline		
			webhook		
ListWebhooks	Grants permission to list all of the webhooks associated with your Amazon Web Services account	List	webhook*		
OverrideStageCondition	Grants permission to resume the pipeline execution by overriding a condition in a stage	Write	stage*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PollForJobs	Grants permission to view information about any jobs for CodePipeline to act on	Write	actiontype*		
PollForThirdPartyJobs	Grants permission to determine whether there are any third-party jobs for a job worker to act on (partner actions only)	Write			
PutActionRevision	Grants permission to edit actions in a pipeline	Write	action*		
PutApprovalResult	Grants permission to provide a response (Approved or Rejected) to a manual approval request in CodePipeline	Write	action*		
PutJobFailureResult	Grants permission to represent the failure of a job as returned to the pipeline by a job worker (custom actions only)	Write			
PutJobSuccessResult	Grants permission to represent the success of a job as returned to the pipeline by a job worker (custom actions only)	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutThirdPartyJobFailureResult	Grants permission to represent the failure of a third-party job as returned to the pipeline by a job worker (partner actions only)	Write			
PutThirdPartyJobSuccessResult	Grants permission to represent the success of a third-party job as returned to the pipeline by a job worker (partner actions only)	Write			
PutWebhook	Grants permission to create or update a webhook	Write	pipeline*		
			webhook*		
				aws:RequestTag/${TagKey} aws:TagKeys	
RegisterWebhookWithThirdParty	Grants permission to register a webhook with the third party specified in its configuration	Write	webhook*		
RetryStageExecution	Grants permission to resume the pipeline execution by retrying the last failed actions in a stage	Write	stage*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RollbackStage	Grants permission to rollback the stage to a previous successful execution	Write	stage*		
StartPipelineExecution	Grants permission to run the most recent revision through the pipeline	Write	pipeline*		
StopPipelineExecution	Grants permission to stop an in-progress pipeline execution	Write	pipeline*		
TagResource	Grants permission to tag a CodePipeline resource	Tagging	actiontype		
			pipeline		
			webhook		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove a tag from a CodePipeline resource	Tagging	actiontype		
			pipeline		
			webhook		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
UpdateActionType	Grants permission to update an action type	Write	actiontype*		
UpdatePipeline	Grants permission to update a pipeline with changes to the structure of the pipeline	Write	pipeline*		

Resource types defined by Amazon CodePipeline

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
action	`arn:${Partition}:codepipeline:${Region}:${Account}:${PipelineName}/${StageName}/${ActionName}`	aws:ResourceTag/${TagKey}
actiontype	`arn:${Partition}:codepipeline:${Region}:${Account}:actiontype:${Owner}/${Category}/${Provider}/${Version}`	aws:ResourceTag/${TagKey}
pipeline	`arn:${Partition}:codepipeline:${Region}:${Account}:${PipelineName}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
stage	`arn:${Partition}:codepipeline:${Region}:${Account}:${PipelineName}/${StageName}`	aws:ResourceTag/${TagKey}
webhook	`arn:${Partition}:codepipeline:${Region}:${Account}:webhook:${WebhookName}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon CodePipeline

Amazon CodePipeline 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 Amazon global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters actions based on the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters actions based on tag key-value pairs attached to the resource	String
aws:TagKeys	Filters actions based on the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Cognito Identity

Amazon Cognito Identity (service prefix: `cognito-identity`) 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 Cognito Identity
- Resource types defined by Amazon Cognito Identity
- Condition keys for Amazon Cognito Identity

Actions defined by Amazon Cognito Identity

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 Amazon. 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.

> **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
CreateIdentityPool	Grants permission to create a new identity pool	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteIdentities	Grants permission to delete identities from an identity pool. You can specify a list of 1-60 identities that you want to delete	Write			
DeleteIdentityPool	Grants permission to delete a user pool. Once a pool is deleted, users will not be able to authenticate with the pool	Write	identitypool*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeIdentity	Grants permission to return metadata related to the given identity, including when the identity was created and any associated linked logins	Read			
DescribeIdentityPool	Grants permission to get details about a particular identity pool, including the pool name, ID description, creation date, and current number of users	Read	identitypool*		
GetCredentialsForIdentity	Grants permission to return credentials for the provided identity ID	Read			
GetId	Grants permission to generate (or retrieve) a Cognito ID. Supplying multiple logins will create an implicit linked account	Write			
GetIdentityPoolAnalytics	Grants permission to get analytics data about the total current identity count for all identity pool identity provider (IdPs)	Read	identitypool*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetIdentityPoolDailyAnalytics	Grants permission to get analytics data about the number of new identities and total identities for all identity pool identity providers (IdPs)	Read	identitypool*		
GetIdentityPoolRoles	Grants permission to get the roles for an identity pool	Read	identitypool*		
GetIdentityProviderDailyAnalytics	Grants permission to get analytics data about the number of new identities and total identities for one identity pool identity provider (IdPs)	Read	identitypool*		
GetOpenIdToken	Grants permission to get an OpenID token, using a known Cognito ID	Read			
GetOpenIdTokenForDeveloperIdentity	Grants permission to register (or retrieve) a Cognito IdentityId and an OpenID Connect token for a user authenticated by your backend authentication process	Read	identitypool*		
GetPrincipalTagAttributeMap	Grants permission to get the principal tags for an identity pool and provider	Read	identitypool*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListIdentities	Grants permission to list the identities in an identity pool	List	identitypool*		
ListIdentityPools	Grants permission to list all of the Cognito identity pools registered for your account	List			
ListTagsForResource	Grants permission to list the tags that are assigned to an Amazon Cognito identity pool	Read	identitypool		
LookupDeveloperIdentity	Grants permission to retrieve the IdentityId associated with a DeveloperUserIdentifier or the list of DeveloperUserIdentifiers associated with an IdentityId for an existing identity	Read	identitypool*		
MergeDeveloperIdentities	Grants permission to merge two users having different IdentityIds, existing in the same identity pool, and identified by the same developer provider	Write	identitypool*		
SetIdentityPoolRoles	Grants permission to set the roles for an identity pool. These roles are used when making calls to GetCredentialsForIdentity action	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SetPrincipalTagAttributeMap	Grants permission to set the principal tags for an identity pool and provider. These tags are used when making calls to GetOpenIdToken action	Write			
TagResource	Grants permission to assign a set of tags to an Amazon Cognito identity pool	Tagging	identitypool		
				aws:RequestTag/${TagKey} aws:TagKeys	
UnlinkDeveloperIdentity	Grants permission to unlink a DeveloperUserIdentifier from an existing identity	Write	identitypool*		
UnlinkIdentity	Grants permission to unlink a federated identity from an existing account	Write			
UntagResource	Grants permission to remove the specified tags from an Amazon Cognito identity pool	Tagging	identitypool		
				aws:TagKeys	
UpdateIdentityPool	Grants permission to update an identity pool	Write	identitypool*		

Resource types defined by Amazon Cognito Identity

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
identitypool	`arn:${Partition}:cognito-identity:${Region}:${Account}:identitypool/${IdentityPoolId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Cognito Identity

Amazon Cognito Identity 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 Amazon global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters actions based on the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters actions based on tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by a key that is present in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Compute Optimizer

Amazon Compute Optimizer (service prefix: `compute-optimizer`) 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 Compute Optimizer
- Resource types defined by Amazon Compute Optimizer
- Condition keys for Amazon Compute Optimizer

Actions defined by Amazon Compute Optimizer

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 Amazon. 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.

> **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
DeleteRecommendationPreferences	Grants permission to delete recommendation preferences	Write		compute-optimizer:ResourceType	autoscaling:DescribeAutoScalingGroups ec2:DescribeInstances rds:DescribeDBClusters

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					rds:DescribeDBInstances
DescribeRecommendationExportJobs	Grants permission to view the status of recommendation export jobs	List			
ExportAutoScalingGroupRecommendations	Grants permission to export AutoScaling group recommendations to S3 for the provided accounts	Write			autoscaling:DescribeAutoScalingGroups compute-optimizer:GetAutoScalingGroupRecommendations
ExportEBSVolumeRecommendations	Grants permission to export EBS volume recommendations to S3 for the provided accounts	Write			compute-optimizer:GetEBSVolumeRecommendations ec2:DescribeVolumes

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ExportEC2InstanceRecommendations	Grants permission to export EC2 instance recommendations to S3 for the provided accounts	Write			compute-optimizer:GetEC2InstanceRecommendations ec2:DescribeInstances
ExportECSServiceRecommendations	Grants permission to export ECS service recommendations to S3 for the provided accounts	Write			compute-optimizer:GetECSServiceRecommendations ecs:ListClusters ecs:ListServices
ExportIdleRecommendations	Grants permission to export idle recommendations to S3 for the provided accounts	Write			compute-optimizer:GetIdleRecommendations

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ExportLambdaFunctionRecommendations	Grants permission to export Lambda function recommendations to S3 for the provided accounts	Write			compute-optimizer:GetLambdaFunctionRecommendations lambda:ListFunctions lambda:ListProvisionedConcurrencyConfigs
ExportLicenseRecommendations	Grants permission to export license recommendations to S3 for the provided account(s)	Write			compute-optimizer:GetLicenseRecommendations ec2:DescribeInstances

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ExportRDSDatabaseRecommendations	Grants permission to export rds recommendations to S3 for the provided accounts	Write			compute-optimizer:GetRDSDatabaseRecommendations rds:DescribeDBClusters rds:DescribeDBInstances
GetAutoScalingGroupRecommendations	Grants permission to get recommendations for the provided AutoScaling groups	List			autoscaling:DescribeAutoScalingGroups
GetEBSVolumeRecommendations	Grants permission to get recommendations for the provided EBS volumes	List			ec2:DescribeVolumes
GetEC2InstanceRecommendations	Grants permission to get recommendations for the provided EC2 instances	List			ec2:DescribeInstances

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetEC2RecommendationProjectedMetrics	Grants permission to get the recommendation projected metrics of the specified instance	List			ec2:DescribeInstances
GetECSServiceRecommendationProjectedMetrics	Grants permission to get the recommendation projected metrics of the specified ECS service	List			
GetECSServiceRecommendations	Grants permission to get recommendations for the provided ECS services	List			ecs:ListClusters ecs:ListServices

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetEffectiveRecommendationPreferences	Grants permission to get recommendation preferences that are in effect	Read		compute-optimizer:ResourceType	autoscaling:DescribeAutoScalingGroups autoscaling:DescribeAutoScalingInstances ec2:DescribeInstances rds:DescribeDBClusters rds:DescribeDBInstances
GetEnrollmentStatus	Grants permission to get the enrollment status for the specified account	List			
GetEnrollmentStatusesForOrganization	Grants permission to get the enrollment statuses for member accounts of the organization	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetIdleRecommendations	Grants permission to get idle recommendations for the specified account(s)	List			
GetLambdaFunctionRecommendations	Grants permission to get recommendations for the provided Lambda functions	List			lambda:ListFunctions lambda:ListProvisionedConcurrencyConfigs
GetLicenseRecommendations	Grants permission to get license recommendations for the specified account(s)	List			ec2:DescribeInstances
GetRDSDatabaseRecommendationProjectedMetrics	Grants permission to get the recommendation projected metrics of the specified instance	List			rds:DescribeDBClusters rds:DescribeDBInstances
GetRDSDatabaseRecommendations	Grants permission to get rds recommendations for the specified account(s)	List			rds:DescribeDBClusters rds:DescribeDBInstances

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRecommendationPreferences	Grants permission to get recommendation preferences	Read		compute-optimizer:ResourceType	
GetRecommendationSummaries	Grants permission to get the recommendation summaries for the specified account(s)	List			
PutRecommendationPreferences	Grants permission to put recommendation preferences	Write		compute-optimizer:ResourceType	autoscaling:DescribeAutoScalingGroups autoscaling:DescribeAutoScalingInstances ec2:DescribeInstances rds:DescribeDBClusters rds:DescribeDBInstances

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateEnrollmentStatus	Grants permission to update the enrollment status	Write			

Resource types defined by Amazon Compute Optimizer

Amazon Compute Optimizer does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon Compute Optimizer, specify `"Resource": "*"` in your policy.

Condition keys for Amazon Compute Optimizer

Amazon Compute Optimizer 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 Amazon global condition context keys.

Condition keys	Description	Type
compute-optimizer:ResourceType	Filters access by the resource type	String

Actions, resources, and condition keys for Amazon Config

Amazon Config (service prefix: `config`) 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 Config
- Resource types defined by Amazon Config
- Condition keys for Amazon Config

Actions defined by Amazon Config

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 Amazon. 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.

> **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
AssociateResourceTypes	Grants permission to add all specified resource types to the RecordingGroup of configuration recorder and includes those resource types when recording	Write	ConfigurationRecorder*		
BatchGetAggregateResourceConfig	Grants permission to return the current configuration items for resources that are present in your Amazon Config aggregator	Read	ConfigurationAggregator*		
BatchGetResourceConfig	Grants permission to return the current configuration for one or more requested resources	Read			
DeleteAggregationAuthorization	Grants permission to delete the authorization granted to the specified configura	Write	AggregationAuthorization*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	tion aggregator account in a specified region				
DeleteConfigRule	Grants permission to delete the specified Amazon Config rule and all of its evaluation results	Write	ConfigRule*		
DeleteConfigurationAggregator	Grants permission to delete the specified configuration aggregator and the aggregated data associated with the aggregator	Write	ConfigurationAggregator*		
DeleteConfigurationRecorder	Grants permission to delete the customer managed configuration recorder	Write	ConfigurationRecorder*		
DeleteConformancePack	Grants permission to delete the specified conformance pack and all the Amazon Config rules and all evaluation results within that conformance pack	Write	ConformancePack*		
DeleteDeliveryChannel	Grants permission to delete the delivery channel	Write			
DeleteEvaluationResults	Grants permission to delete the evaluation results for the specified Config rule	Write	ConfigRule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteOrganizationConfigRule	Grants permission to delete the specified organization config rule and all of its evaluation results from all member accounts in that organization	Write	OrganizationConfigRule*		
DeleteOrganizationConformancePack	Grants permission to delete the specified organization conformance pack and all of its evaluation results from all member accounts in that organization	Write	OrganizationConformancePack*		
DeletePendingAggregationRequest	Grants permission to delete pending authorization requests for a specified aggregator account in a specified region	Write			
DeleteRemediationConfiguration	Grants permission to delete the remediation configuration	Write	RemediationConfiguration*		
DeleteRemediationExceptions	Grants permission to delete one or more remediation exceptions for specific resource keys for a specific Amazon Config Rule	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteResourceConfig	Grants permission to record the configuration state for a custom resource that has been deleted	Write			
DeleteRetentionConfiguration	Grants permission to delete the retention configuration	Write			
DeleteServiceLinkedConfigurationRecorder	Grants permission to delete the service-linked configuration recorder	Write	ConfigurationRecorder*		
				config:ConfigurationRecorderServicePrincipal	
DeleteStoredQuery	Grants permission to delete the stored query for an Amazon Web Services account in an Amazon Web Services Region	Write	StoredQuery*		
DeliverConfigSnapshot	Grants permission to schedule delivery of a configuration snapshot to the Amazon S3 bucket in the specified delivery channel	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeAggregateComplianceByConfigRules	Grants permission to return a list of compliant and noncompliant rules with the number of resources for compliant and noncompliant rules	Read	ConfigurationAggregator*		
DescribeAggregateComplianceByConformancePacks	Grants permission to return a list of compliant and noncompliant conformance packs along with count of compliant, non-compliant and total rules within each conformance pack	Read	ConfigurationAggregator*		
DescribeAggregationAuthorizations	Grants permission to return a list of authorizations granted to various aggregator accounts and regions	List			
DescribeComplianceByConfigRule	Grants permission to indicate whether the specified Amazon Config rules are compliant	Read			
DescribeComplianceByResource	Grants permission to indicate whether the specified Amazon resources are compliant	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeConfigRuleEvaluationStatus	Grants permission to return status information for each of your Amazon managed Config rules	Read			
DescribeConfigRules	Grants permission to return details about your Amazon Config rules	List			
DescribeConfigurationAggregatorSourcesStatus	Grants permission to return status information for sources within an aggregator	Read	ConfigurationAggregator*		
DescribeConfigurationAggregators	Grants permission to return the details of one or more configuration aggregators	List			
DescribeConfigurationRecorderStatus	Grants permission to return the current status of the specified configuration recorder	Read	ConfigurationRecorder*		
				config:ConfigurationRecorderServicePrincipal	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeConfigurationRecorders	Grants permission to return the names of one or more specified configuration recorders	Read	ConfigurationRecorder*		
				config:ConfigurationRecorderServicePrincipal	
DescribeConformancePackCompliance	Grants permission to return compliance information for each rule in that conformance pack	Read	ConformancePack*		
DescribeConformancePackStatus	Grants permission to provide one or more conformance packs deployment status	Read			
DescribeConformancePacks	Grants permission to return a list of one or more conformance packs	List			
DescribeDeliveryChannelStatus	Grants permission to return the current status of the specified delivery channel	Read			
DescribeDeliveryChannels	Grants permission to return details about the specified delivery channel	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeOrganizationConfigRuleStatuses	Grants permission to provide organization config rule deployment status for an organization	Read			
DescribeOrganizationConfigRules	Grants permission to return a list of organization config rules	List			
DescribeOrganizationConformancePackStatuses	Grants permission to provide organization conformance pack deployment status for an organization	Read			
DescribeOrganizationConformancePacks	Grants permission to return a list of organization conformance packs	List			
DescribePendingAggregationRequests	Grants permission to return a list of all pending aggregation requests	List			
DescribeRemediationConfigurations	Grants permission to return the details of one or more remediation configurations	List	RemediationConfiguration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeRemediationExceptions	Grants permission to return the details of one or more remediation exceptions	List			
DescribeRemediationExecutionStatus	Grants permission to provide a detailed view of a Remediation Execution for a set of resources including state, timestamps and any error messages for steps that have failed	Read	RemediationConfiguration*		
DescribeRetentionConfigurations	Grants permission to return the details of one or more retention configurations	List			
DisassociateResourceTypes	Grants permission to remove all specified resource types from the RecordingGroup of configuration recorder and excludes these resource types when recording	Write	ConfigurationRecorder*		
GetAggregateComplianceDetailsByConfigRule	Grants permission to return the evaluation results for the specified Amazon Config rule for a specific resource in a rule	Read	ConfigurationAggregator*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAggregateConfigRuleComplianceSummary	Grants permission to return the number of compliant and noncompliant rules for one or more accounts and regions in an aggregator	Read	ConfigurationAggregator*		
GetAggregateConformancePackComplianceSummary	Grants permission to return the number of compliant and noncompliant conformance packs for one or more accounts and regions in an aggregator	Read	ConfigurationAggregator*		
GetAggregateDiscoveredResourceCounts	Grants permission to return the resource counts across accounts and regions that are present in your Amazon Config aggregator	Read	ConfigurationAggregator*		
GetAggregateResourceConfig	Grants permission to return configuration item that is aggregated for your specific resource in a specific source account and region	Read	ConfigurationAggregator*		
GetComplianceDetailsByConfigRule	Grants permission to return the evaluation results for the specified Amazon Config rule	Read	ConfigRule*		
GetComplianceDetailsByResource	Grants permission to return the evaluation results for the specified Amazon resource	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetComplianceSummaryByConfigRule	Grants permission to return the number of Amazon Config rules that are compliant and noncompliant, up to a maximum of 25 for each	Read			
GetComplianceSummaryByResourceType	Grants permission to return the number of resources that are compliant and the number that are noncompliant	Read			
GetConformancePackComplianceDetails	Grants permission to return compliance details of a conformance pack for all Amazon resources that are monitered by conformance pack	Read	ConformancePack*		
GetConformancePackComplianceSummary	Grants permission to provide compliance summary for one or more conformance packs	Read	ConformancePack*		
GetCustomRulePolicy	Grants permission to return the policy definition containing the logic for your Amazon Config Custom Policy rule	Read	ConfigRule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDiscoveredResourceCounts	Grants permission to return the resource types, the number of each resource type, and the total number of resources that Amazon Config is recording in this region for your Amazon Web Services account	Read			
GetOrganizationConfigRuleDetailedStatus	Grants permission to return detailed status for each member account within an organization for a given organization config rule	Read	OrganizationConfigRule*		
GetOrganizationConformancePackDetailedStatus	Grants permission to return detailed status for each member account within an organization for a given organization conformance pack	Read	OrganizationConformancePack*		
GetOrganizationCustomRulePolicy	Grants permission to return the policy definition containing the logic for your organization Amazon Config Custom Policy rule	Read	OrganizationConfigRule*		
GetResourceConfigHistory	Grants permission to return a list of configuration items for the specified resource	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetResourceEvaluationSummary	Grants permission to return the summary of resource evaluations for a specific resource evaluation ID	Read			
GetStoredQuery	Grants permission to return the details of a specific stored query	Read	StoredQuery*		
ListAggregateDiscoveredResources	Grants permission to accept a resource type and returns a list of resource identifiers that are aggregated for a specific resource type across accounts and regions	List	ConfigurationAggregator*		
ListConfigurationRecorders	Grants permission to list the configuration recorder summaries for an Amazon Web Services account in an Amazon Web Services Region	List			
ListConformancePackComplianceScores	Grants permission to return the percentage of compliant rule-resource combinations in a conformance pack compared to the number of total possible rule-resource combinations	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDiscoveredResources	Grants permission to accept a resource type and returns a list of resource identifiers for the resources of that type	List			
ListResourceEvaluations	Grants permission to list the resource evaluation summaries for an Amazon Web Services account in an Amazon Web Services Region	List			
ListStoredQueries	Grants permission to list the stored queries for an Amazon Web Services account in an Amazon Web Services Region	List			
ListTagsForResource	Grants permission to list the tags for Amazon Config resource	Read	AggregationAuthorization		
			ConfigRule		
			ConfigurationAggregator		
			ConfigurationRecorder		
			ConformancePack		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			OrganizationConfigRule		
			OrganizationConformancePack		
			StoredQuery		
PutAggregationAuthorization	Grants permission to authorize the aggregator account and region to collect data from the source account and region	Write	AggregationAuthorization*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PutConfigRule	Grants permission to add or update an Amazon Config rule for evaluating whether your Amazon resources comply with your desired configurations	Write	ConfigRule*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutConfigurationAggregator	Grants permission to create and update the configuration aggregator with the selected source accounts and regions	Write	ConfigurationAggregator*		iam:PassRole organizations:EnableAWSServiceAccess organizations:ListDelegatedAdministrators
				aws:RequestTag/${TagKey} aws:TagKeys	
PutConfigurationRecorder	Grants permission to create or update a customer managed configuration recorder to record the selected resource configurations	Write	ConfigurationRecorder*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutConformancePack	Grants permission to create or update a conformance pack	Write	ConformancePack*		iam:CreateServiceLinkedRole iam:PassRole s3:GetObject s3:ListBucket ssm:GetDocument
PutDeliveryChannel	Grants permission to create a delivery channel object to deliver configuration information to an Amazon S3 bucket and Amazon SNS topic	Write			
PutEvaluations	Grants permission to be used by an Amazon Lambda function to deliver evaluation results to Amazon Config	Write			
PutExternalEvaluation	Grants permission to deliver evaluation result to Amazon Config	Write	ConfigRule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutOrganizationConfigRule	Grants permission to add or update organization config rule for your entire organization evaluating whether your Amazon resources comply with your desired configurations	Write	OrganizationConfigRule*		iam:CreateServiceLinkedRole iam:PassRole organizations:EnableAWSServiceAccess organizations:ListDelegatedAdministrators

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutOrganizationConformancePack	Grants permission to add or update organization conformance pack for your entire organization evaluating whether your Amazon resources comply with your desired configurations	Write	OrganizationConformancePack*		iam:CreateServiceLinkedRole iam:PassRole organizations:EnableAWSServiceAccess organizations:ListDelegatedAdministrators s3:GetObject
PutRemediationConfigurations	Grants permission to add or update the remediation configuration with a specific Amazon Config rule with the selected target or action	Write	RemediationConfiguration*		iam:PassRole
PutRemediationExceptions	Grants permission to add or update remediation exceptions for specific resources for a specific Amazon Config rule	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutResourceConfig	Grants permission to record the configuration state for the resource provided in the request	Write			
PutRetentionConfiguration	Grants permission to create and update the retention configuration with details about retention period (number of days) that Amazon Config stores your historical information	Write			
PutServiceLinkedConfigurationRecorder	Grants permission to create a new service-linked configuration recorder to record the resource configurations in scope for the linked service	Write		aws:RequestTag/${TagKey} aws:TagKeys config:ConfigurationRecorderServicePrincipal	iam:CreateServiceLinkedRole iam:PassRole
PutStoredQuery	Grants permission to save a new query or updates an existing saved query	Write	StoredQuery*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
SelectAggregateResourceConfig	Grants permission to accept a structured query language (SQL) SELECT command and an aggregator to query configuration state of Amazon resources across multiple accounts and regions, performs the corresponding search, and returns resource configurations matching the properties	Read	ConfigurationAggregator*		
SelectResourceConfig	Grants permission to accept a structured query language (SQL) SELECT command, performs the corresponding search, and returns resource configurations matching the properties	Read			
StartConfigRulesEvaluation	Grants permission to evaluate your resources against the specified Config rules	Write	ConfigRule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartConfigurationRecorder	Grants permission to the customer managed configuration recorder to start recording configurations of the Amazon resources you have selected to record in your Amazon Web Services account	Write	ConfigurationRecorder*		
StartRemediationExecution	Grants permission to run an on-demand remediation for the specified Amazon Config rules against the last known remediation configuration	Write			iam:PassRole
StartResourceEvaluation	Grants permission to evaluate your resource details against the Amazon Config rules in your account	Write			cloudformation:DescribeType
StopConfigurationRecorder	Grants permission to the customer managed configuration recorder to stop recording configurations of the Amazon resources you have selected to record in your Amazon Web Services account	Write	ConfigurationRecorder*		
TagResource	Grants permission to associate the specified tags to a resource with the specified resourceArn	Tagging	AggregationAuthorization		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ConfigRule		
			ConfigurationAggregator		
			ConfigurationRecorder		
			ConformancePack		
			OrganizationConfigRule		
			OrganizationConformancePack		
			StoredQuery		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagResource	Grants permission to delete specified tags from a resource	Tagging	AggregationAuthorization		
			ConfigRule		
			ConfigurationAggregator		
			ConfigurationRecorder		
			ConformancePack		
			OrganizationConfigRule		
			OrganizationConformancePack		
			StoredQuery		
				aws:TagKeys	

Resource types defined by Amazon Config

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
AggregationAuthorization	`arn:${Partition}:config:${Region}:${Account}:aggregation-authorization/${AggregatorAccount}/${AggregatorRegion}`	aws:ResourceTag/${TagKey}
ConfigurationAggregator	`arn:${Partition}:config:${Region}:${Account}:config-aggregator/${AggregatorId}`	aws:ResourceTag/${TagKey}
ConfigRule	`arn:${Partition}:config:${Region}:${Account}:config-rule/${ConfigRuleId}`	aws:ResourceTag/${TagKey}
ConformancePack	`arn:${Partition}:config:${Region}:${Account}:conformance-pack/${ConformancePackName}/${ConformancePackId}`	aws:ResourceTag/${TagKey}
OrganizationConfigRule	`arn:${Partition}:config:${Region}:${Account}:organization-config-rule/${OrganizationConfigRuleId}`	aws:ResourceTag/${TagKey}
OrganizationConformancePack	`arn:${Partition}:config:${Region}:${Account}:organization-conformance-pack/${OrganizationConformancePackId}`	aws:ResourceTag/${TagKey}
RemediationConfiguration	`arn:${Partition}:config:${Region}:${Account}:remediation-configuration/${RemediationConfigurationId}`	

Resource types	ARN	Condition keys
StoredQuery	`arn:${Partition}:config:${Region}:${Account}:stored-query/${StoredQueryName}/${StoredQueryId}`	aws:ResourceTag/${TagKey}
ConfigurationRecorder	`arn:${Partition}:config:${Region}:${Account}:configuration-recorder/${RecorderName}/${RecorderId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Config

Amazon Config 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 Amazon 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
config:ConfigurationRecorderServicePrincipal	Filters access by service principal of the configuration recorder	String

Actions, resources, and condition keys for Amazon Connector Service

Amazon Connector Service (service prefix: `awsconnector`) 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 Connector Service
- Resource types defined by Amazon Connector Service
- Condition keys for Amazon Connector Service

Actions defined by Amazon Connector 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 Amazon. 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.

> **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
GetConnectorHealth [permission only]	Retrieves all health metrics that were published from the Server Migration Connector.	Read			
RegisterConnector [permission only]	Registers Amazon Connector with Amazon Connector Service.	Write			
ValidateConnectorId [permission only]	Validates Server Migration Connector Id that was registered with Amazon Connector Service.	Read			

Resource types defined by Amazon Connector Service

Amazon Connector Service does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon Connector Service, specify `"Resource": "*"` in your policy.

Condition keys for Amazon Connector Service

Connector Service 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 Amazon global condition context keys.

Actions, resources, and condition keys for Amazon Consolidated Billing

Amazon Consolidated Billing (service prefix: `consolidatedbilling`) 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 Consolidated Billing
- Resource types defined by Amazon Consolidated Billing
- Condition keys for Amazon Consolidated Billing

Actions defined by Amazon Consolidated Billing

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 Amazon. 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.

> **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
GetAccountBillingRole [permission only]	Grants permission to get account role (Payer, Linked, Regular)	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListLinkedAccounts [permission only]	Grants permission to get list of member/linked accounts	List			

Resource types defined by Amazon Consolidated Billing

Amazon Consolidated Billing does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon Consolidated Billing, specify `"Resource": "*"` in your policy.

Condition keys for Amazon Consolidated Billing

Consolidated Billing 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 Amazon global condition context keys.

Actions, resources, and condition keys for Amazon Cost and Usage Report

Amazon Cost and Usage Report (service prefix: `cur`) 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 Cost and Usage Report

- Resource types defined by Amazon Cost and Usage Report
- Condition keys for Amazon Cost and Usage Report

Actions defined by Amazon Cost and Usage Report

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 Amazon. 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.

> **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
DeleteReportDefinition	Grants permission to delete Cost and Usage Report Definition	Write	cur*		
DescribeReportDefinitions	Grants permission to get Cost and Usage Report Definitions	Read			
GetClassicReport [permission only]	Grants permission to get Bills CSV report	Read			
GetClassicReportPreferences [permission only]	Grants permission to get the classic report enablement status for Usage Reports	Read			
GetUsageReport [permission only]	Grants permission to get list of Amazon services, usage type and operation for the Usage Report workflow. Allows or denies download of usage reports too	Read			
ListTagsForResource	Grants permission to list tags for a resource	Read	cur*		
				aws:ResourceTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey}	
ModifyReportDefinition	Grants permission to modify Cost and Usage Report Definition	Write	cur*		
PutClassicReportPreferences [permission only]	Grants permission to enable classic reports	Write			
PutReportDefinition	Grants permission to write Cost and Usage Report Definition	Write	cur*		
TagResource	Grants permission to tag a resource	Tagging	cur*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to untag a resource	Tagging	cur*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:ResourceTag/${TagKey}	
ValidateReportDestination [permission only]	Grants permission to validates if the s3 bucket exists with appropriate permissions for CUR delivery	Read			

Resource types defined by Amazon Cost and Usage Report

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
cur	`arn:${Partition}:cur:${Region}:${Account}:definition/${ReportName}`	

Condition keys for Amazon Cost and Usage Report

Amazon Cost and Usage Report 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 Amazon 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 Cost Explorer Service

Amazon 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 Amazon Cost Explorer Service

- Resource types defined by Amazon Cost Explorer Service
- Condition keys for Amazon Cost Explorer Service

Actions defined by Amazon 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 Amazon. 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.

> **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	
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateReport [permission only]	Grants permission to create Cost Explorer Reports	Write			
DeleteAnomalyMonitor	Grants permission to delete an Anomaly Monitor	Write	anomalymonitor*		
				aws:ResourceTag/${TagKey}	
DeleteAnomalySubscription	Grants permission to delete an Anomaly Subscription	Write	anomalysubscription*		
				aws:ResourceTag/${TagKey}	
DeleteCostCategoryDefinition	Grants permission to delete a Cost Category	Write	costcategory*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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}	
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
GetAnomalyMonitors	Grants permission to query Anomaly Monitors	Read	anomalymonitor*		
				aws:ResourceTag/${TagKey}	
GetAnomalySubscriptions	Grants permission to query Anomaly Subscriptions	Read	anomalysubscription*		
				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			

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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
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			
StartCommitmentPurchaseAnalysis	Grants permission to request a commitment purchase analysis	Write			
StartCostAllocationTagBackfill	Grants permission to request a Cost Allocation Tag backfill	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartSavingsPlansPurchaseRecommendationGeneration	Grants permission to request a Savings Plans recommendation generation	Write			
TagResource	Grants permission to tag a Cost Explorer resource	Tagging	anomalymonitor		
			anomalysubscription		
			costcategory		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to remove tags from a Cost Explorer resource	Tagging	anomalymonitor		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			anomalysubscription		
			costcategory		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateAnomalyMonitor	Grants permission to update an existing Anomaly Monitor	Write	anomalymonitor*		
				aws:ResourceTag/${TagKey}	
UpdateAnomalySubscription	Grants permission to update an existing Anomaly Subscription	Write	anomalysubscription*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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}	
UpdateNotificationSubscription [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 Amazon 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}
costcategory	`arn:${Partition}:ce::${Account}:costcategory/${Identifier}`	aws:ResourceTag/${TagKey}
billingview	`arn:${Partition}:billing::${Account}:billingview/${ResourceId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Cost Explorer Service

Amazon 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 Amazon 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

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 Amazon. 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.

> **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	Write		aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Amazon EBS snapshots. You may have up to 100 policies			aws:TagKeys	
DeleteLifecyclePolicy	Grants permission to delete an existing data lifecycle policy. In addition, this action halts the creation and deletion of snapshots that the policy specified. Existing snapshots are not affected	Write	policy*		
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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 Amazon 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 Amazon Database Migration Service

Amazon Database Migration Service (service prefix: `dms`) 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 Database Migration Service
- Resource types defined by Amazon Database Migration Service
- Condition keys for Amazon Database Migration Service

Actions defined by Amazon Database Migration 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 Amazon. 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.

> **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
AddTagsToResource	Grants permission to add metadata tags to DMS resources, including replication instances, endpoints, security groups, and migration tasks	Tagging	Certificate		
			DataMigration		
			DataProvider		
			Endpoint		
			EventSubscription		
			InstanceProfile		
			MigrationProject		
			ReplicationConfig		
			ReplicationInstance		
			ReplicationSubnetGroup		
			ReplicationTask		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ReplicationTaskAssessmentRun		
			ReplicationTaskIndividualAssessment		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
ApplyPendingMaintenanceAction	Grants permission to apply a pending maintenance action to a resource (for example, to a replication instance)	Write	ReplicationInstance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateExtensionPack	Grants permission to associate a extension pack	Write	MigrationProject*		
BatchStartRecommendations	Grants permission to start the analysis of up to 20 source databases to recommend target engines for each source database	Write			
CancelReplicationTaskAssessmentRun	Grants permission to cancel a single premigration assessment run	Write	ReplicationTaskAssessmentRun*		
CreateDataMigration	Grants permission to create a database migration using the provided settings	Write	MigrationProject*		iam:PassRole

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDataProvider	Grants permission to create an data provider using the provided settings	Write		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateEndpoint	Grants permission to create an endpoint using the provided settings	Write		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateEventSubscription	Grants permission to create an Amazon DMS event notification subscription	Write		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
CreateFleetAdvisorCollector	Grants permission to create a Fleet Advisor collector using the specified parameters	Write			iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateInstanceProfile	Grants permission to create an instance profile using the provided settings	Write		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	iam:PassRole
CreateMigrationProject	Grants permission to create an migration project using the provided settings	Write	DataProvider* InstanceProfile*		iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
CreateReplicationConfig	Grants permission to create a replication config using the provided settings	Write	Endpoint*		

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateReplicationInstance	Grants permission to create a replication instance using the specified parameters	Write		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateReplicationSubnetGroup	Grants permission to create a replication subnet group given a list of the subnet IDs in a VPC	Write		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
CreateReplicationTask	Grants permission to create a replication task using the specified parameters	Write	Endpoint*		
			ReplicationInstance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys dms:req-tag/${TagKey}	
DeleteCertificate	Grants permission to delete the specified certificate	Write	Certificate*		
DeleteConnection	Grants permission to delete the specified connection between a replication instance and an endpoint	Write	Endpoint*		
			ReplicationInstance*		
DeleteDataMigration	Grants permission to delete the specified database migration	Write	DataMigration*		
DeleteDataProvider	Grants permission to delete the specified data provider	Write	DataProvider*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteEndpoint	Grants permission to delete the specified endpoint	Write	Endpoint*		
DeleteEventSubscription	Grants permission to delete an Amazon DMS event subscription	Write	EventSubscription*		
DeleteFleetAdvisorCollector	Grants permission to delete the specified Fleet Advisor collector	Write			
DeleteFleetAdvisorDatabases	Grants permission to delete the specified Fleet Advisor databases	Write			
DeleteInstanceProfile	Grants permission to delete the specified instance profile	Write	InstanceProfile*		
DeleteMigrationProject	Grants permission to delete the specified migration project	Write	MigrationProject*		
DeleteReplicationConfig	Grants permission to delete the specified replication config	Write	ReplicationConfig*		
DeleteReplicationInstance	Grants permission to delete the specified replication instance	Write	ReplicationInstance*		
DeleteReplicationSubnetGroup	Grants permission to deletes a subnet group	Write	ReplicationSubnetGroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteReplicationTask	Grants permission to delete the specified replication task	Write	ReplicationTask*		
DeleteReplicationTaskAssessmentRun	Grants permission to delete the record of a single premigration assessment run	Write	ReplicationTaskAssessmentRun*		
DescribeAccountAttributes	Grants permission to list all of the Amazon DMS attributes for a customer account	Read			
DescribeApplicableIndividualAssessments	Grants permission to list individual assessments that you can specify for a new premigration assessment run	Read	ReplicationInstance		
			ReplicationTask		
DescribeCertificates	Grants permission to provide a description of the certificate	Read			
DescribeConnections	Grants permission to describe the status of the connections that have been made between the replication instance and an endpoint	Read			
DescribeConversionConfiguration	Grants permission to return information about DMS Schema Conversion project configuration	Read	MigrationProject*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDataMigrations	Grants permission to return information about database migrations for your account in the specified region	Read			
DescribeEndpointSettings	Grants permission to return the possible endpoint settings available when you create an endpoint for a specific database engine	Read			
DescribeEndpointTypes	Grants permission to return information about the type of endpoints available	Read			
DescribeEndpoints	Grants permission to return information about the endpoints for your account in the current region	Read			
DescribeEngineVersions	Grants permission to return information about the available versions for DMS replication instances	Read			
DescribeEventCategories	Grants permission to list categories for all event source types, or, if specified, for a specified source type	Read			
DescribeEventSubscriptions	Grants permission to list all the event subscriptions for a customer account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeEvents	Grants permission to list events for a given source identifier and source type	Read			
DescribeFleetAdvisorCollectors	Grants permission to return a paginated list of Fleet Advisor collectors in your account based on filter settings	Read			
DescribeFleetAdvisorDatabases	Grants permission to return a paginated list of Fleet Advisor databases in your account based on filter settings	Read			
DescribeFleetAdvisorLsaAnalysis	Grants permission to return a paginated list of descriptions of large-scale assessment (LSA) analyses produced by your Fleet Advisor collectors	Read			
DescribeFleetAdvisorSchemaObjectSummary	Grants permission to return a paginated list of descriptions of schemas discovered by your Fleet Advisor collectors based on filter settings	Read			
DescribeFleetAdvisorSchemas	Grants permission to return a paginated list of schemas discovered by your Fleet Advisor collectors based on filter settings	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeMetadataModelImports	Grants permission to return information about start metadata model import operations for a migration project	Read	Migration Project*		
DescribeOrderableReplicationInstances	Grants permission to return information about the replication instance types that can be created in the specified region	Read			
DescribePendingMaintenanceActions	Grants permission to return information about pending maintenance actions	Read			
DescribeRecommendationLimitations	Grants permission to return a paginated list of descriptions of limitations for recommendations of target Amazon engines	Read			
DescribeRecommendations	Grants permission to return a paginated list of descriptions of target engine recommendations for your source databases	Read			
DescribeRefreshSchemasStatus	Grants permission to returns the status of the RefreshSchemas operation	Read	Endpoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeReplicationConfigs	Grants permission to describe replication configs	Read			
DescribeReplicationInstanceTaskLogs	Grants permission to return information about the task logs for the specified task	Read	ReplicationInstance*		
				aws:ResourceTag/${TagKey} aws:TagKeys	
DescribeReplicationInstances	Grants permission to return information about replication instances for your account in the current region	Read			
DescribeReplicationSubnetGroups	Grants permission to return information about the replication subnet groups	Read			
DescribeReplicationTableStatistics	Grants permission to describe replication table statistics	Read	ReplicationConfig*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeReplicationTaskAssessmentResults	Grants permission to return the latest task assessment results from Amazon S3	Read	ReplicationTask		
DescribeReplicationTaskAssessmentRuns	Grants permission to return a paginated list of premigration assessment runs based on filter settings	Read	ReplicationInstance		
			ReplicationTask		
			ReplicationTaskAssessmentRun		
DescribeReplicationTaskIndividualAssessments	Grants permission to return a paginated list of individual assessments based on filter settings	Read	ReplicationTask		
			ReplicationTaskAssessmentRun		
DescribeReplicationTasks	Grants permission to return information about replication tasks for your account in the current region	Read			
DescribeReplications	Grants permission to describe replications	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeSchemas	Grants permission to return information about the schema for the specified endpoint	Read	Endpoint*		
DescribeTableStatistics	Grants permission to return table statistics on the database migration task, including table name, rows inserted, rows updated, and rows deleted	Read	ReplicationTask*		
ExportMetadataModelAssessment	Grants permission to export the specified metadata model assessment	Write	MigrationProject		
ImportCertificate	Grants permission to upload the specified certificate	Write		aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
ListDataProviders	Grants permission to list the Amazon DMS attributes for a data providers	Read	DataProvider		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListExtensionPacks	Grants permission to list the Amazon DMS attributes for a extension packs	Read	Migration Project		
ListInstanceProfiles	Grants permission to list the Amazon DMS attributes for a instance profiles	Read	InstanceProfile		
ListMetadataModelAssessmentActionItems [permission only]	Grants permission to list the Amazon DMS attributes for a metadata model assessment action items. Note. Despite this action requires StartMetadataModelImport, the latter does not currently authorize the described Schema Conversion operation	Read	Migration Project		dms:StartMetadataModelImport
ListMetadataModelAssessments	Grants permission to list the Amazon DMS attributes for a metadata model assessments	Read	Migration Project		
ListMetadataModelConversions	Grants permission to list the Amazon DMS attributes for a metadata model conversions	Read	Migration Project		
ListMetadataModelExports	Grants permission to list the Amazon DMS attributes for a metadata model exports	Read	Migration Project		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListMigrationProjects	Grants permission to list the Amazon DMS attributes for a migration projects. Note. Despite this action requires DescribeMigrationProjects and DescribeConversion Configuration, both required actions do not currently authorize the described Schema Conversion operation	Read	DataProvider		dms:DescribeConversionConfiguration
			InstanceProfile		
			MigrationProject		
ListTagsForResource	Grants permission to list all tags for an Amazon DMS resource	Read	Certificate		
			DataMigration		
			DataProvider		
			Endpoint		
			EventSubscription		
			InstanceProfile		
			MigrationProject		
			ReplicationConfig		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ReplicationInstance		
			ReplicationSubnetGroup		
			ReplicationTask		
			ReplicationTaskAssessmentRun		
			ReplicationTaskIndividualAssessment		
ModifyDataMigration	Grants permission to modify the specified database migration	Write	DataMigration*		iam:PassRole
ModifyEndpoint	Grants permission to modify the specified endpoint	Write	Endpoint*		iam:PassRole
			Certificate		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyEventSubscription	Grants permission to modify an existing Amazon DMS event notification subscription	Write			
ModifyFleetAdvisorCollector [permission only]	Grants permission to modify the name and description of the specified Fleet Advisor collector	Write			
ModifyFleetAdvisorCollectorStatuses [permission only]	Grants permission to modify the status of the specified Fleet Advisor collector	Write			
ModifyReplicationConfig	Grants permission to modify the specified replication config	Write	ReplicationConfig*		
ModifyReplicationInstance	Grants permission to modify the replication instance to apply new settings	Write	ReplicationInstance*		
ModifyReplicationSubnetGroup	Grants permission to modify the settings for the specified replication subnet group	Write			
ModifyReplicationTask	Grants permission to modify the specified replication task	Write	ReplicationTask*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
MoveReplicationTask	Grants permission to move the specified replication task to a different replication instance	Write	ReplicationInstance*		
			ReplicationTask*		
RebootReplicationInstance	Grants permission to reboot a replication instance. Rebooting results in a momentary outage, until the replication instance becomes available again	Write	ReplicationInstance*		
RefreshSchemas	Grants permission to populate the schema for the specified endpoint	Write	Endpoint*		
			ReplicationInstance*		
ReloadReplicationTables	Grants permission to reload the target database table with the source for a replication	Write	ReplicationConfig*		
ReloadTables	Grants permission to reload the target database table with the source data	Write	ReplicationTask*		
RemoveTagsFromResource	Grants permission to remove metadata tags from a DMS resource	Tagging	Certificate		
			DataMigration		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			DataProvider		
			Endpoint		
			EventSubscription		
			InstanceProfile		
			MigrationProject		
			ReplicationConfig		
			ReplicationInstance		
			ReplicationSubnetGroup		
			ReplicationTask		
			ReplicationTaskAssessmentRun		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ReplicationTaskIndividualAssessment		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
RunFleetAdvisorLsaAnalysis	Grants permission to run a large-scale assessment (LSA) analysis on every Fleet Advisor collector in your account	Write			
StartDataMigration	Grants permission to start the database migration	Write	DataMigration*		
StartMetadataModelAssessment	Grants permission to start a new assessment of metadata model	Write	MigrationProject*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartMetadataModelConversion	Grants permission to start a new conversion of metadata model	Write	MigrationProject*		
StartMetadataModelExportAsScripts	Grants permission to start a new export of metadata model as script	Write	MigrationProject*		
StartMetadataModelExportToTarget	Grants permission to start a new export of metadata model to target	Write	MigrationProject*		
StartMetadataModelImport	Grants permission to start a new import of metadata model	Write	MigrationProject*		
StartRecommendations	Grants permission to start the analysis of your source database to provide recommendations of target engines	Write			
StartReplication	Grants permission to start a replication	Write	ReplicationConfig*		
StartReplicationTask	Grants permission to start the replication task	Write	ReplicationTask*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartReplicationTaskAssessment	Grants permission to start the replication task assessment for unsupported data types in the source database	Write	ReplicationTask*		
StartReplicationTaskAssessmentRun	Grants permission to start a new premigration assessment run for one or more individual assessments of a migration task	Write	ReplicationTask*		iam:PassRole
StopDataMigration	Grants permission to stop the database migration	Write	DataMigration*		
StopReplication	Grants permission to stop a replication	Write	ReplicationConfig*		
StopReplicationTask	Grants permission to stop the replication task	Write	ReplicationTask*		
TestConnection	Grants permission to test the connection between the replication instance and the endpoint	Read	Endpoint*		
			ReplicationInstance*		
UpdateConversionConfiguration	Grants permission to update a conversion configuration	Write	MigrationProject*		
UpdateDataProvider	Grants permission to update the specified data provider	Write	DataProvider*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateInstanceProfile	Grants permission to update the specified instance profile	Write	InstanceProfile*		
UpdateMigrationProject	Grants permission to update the specified migration project	Write	MigrationProject*		
UpdateSubscriptionsToEventBridge	Grants permission to migrate DMS subcriptions to Eventbridge	Write			
UploadFileMetadataList [permission only]	Grants permission to upload files to your Amazon S3 bucket	Write			

Resource types defined by Amazon Database Migration 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
Certificate	`arn:${Partition}:dms:${Region}:${Account}:cert:*`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
		dms:cert-tag/${TagKey}
DataProvider	arn:${Partition}:dms:${Region}:${Account}:data-provider:*	aws:ResourceTag/${TagKey} dms:data-provider-tag/${TagKey}
DataMigration	arn:${Partition}:dms:${Region}:${Account}:data-migration:*	aws:ResourceTag/${TagKey} dms:data-migration-tag/${TagKey}
Endpoint	arn:${Partition}:dms:${Region}:${Account}:endpoint:*	aws:ResourceTag/${TagKey} dms:endpoint-tag/${TagKey}
EventSubscription	arn:${Partition}:dms:${Region}:${Account}:es:*	aws:ResourceTag/${TagKey} dms:es-tag/${TagKey}
InstanceProfile	arn:${Partition}:dms:${Region}:${Account}:instance-profile:*	aws:ResourceTag/${TagKey} dms:instance-profile-tag/${TagKey}

Resource types	ARN	Condition keys
Migration Project	`arn:${Partition}:dms:${Region}:${Account}:migration-project:*`	aws:ResourceTag/${TagKey} dms:migration-project-tag/${TagKey}
ReplicationConfig	`arn:${Partition}:dms:${Region}:${Account}:replication-config:*`	aws:ResourceTag/${TagKey} dms:replication-config-tag/${TagKey}
ReplicationInstance	`arn:${Partition}:dms:${Region}:${Account}:rep:*`	aws:ResourceTag/${TagKey} dms:rep-tag/${TagKey}
ReplicationSubnetGroup	`arn:${Partition}:dms:${Region}:${Account}:subgrp:*`	aws:ResourceTag/${TagKey} dms:subgrp-tag/${TagKey}
ReplicationTask	`arn:${Partition}:dms:${Region}:${Account}:task:*`	aws:ResourceTag/${TagKey} dms:task-tag/${TagKey}
ReplicationTaskAssessmentRun	`arn:${Partition}:dms:${Region}:${Account}:assessment-run:*`	aws:ResourceTag/${TagKey} dms:assessment-run-tag/${TagKey}

Resource types	ARN	Condition keys
ReplicationTaskIndividualAssessment	`arn:${Partition}:dms:${Region}:${Account}:individual-assessment:*`	aws:ResourceTag/${TagKey} dms:individual-assessment-tag/${TagKey}

Condition keys for Amazon Database Migration Service

Amazon Database Migration 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 Amazon 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 the presence of tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString
dms:assessment-run-tag/${TagKey}	Filters access by the presence of tag key-value pairs in the request for AssessmentRun	String
dms:cert-tag/${TagKey}	Filters access by the presence of tag key-value pairs in the request for Certificate	String

Condition keys	Description	Type
dms:data-migration-tag/${TagKey}	Filters access by the presence of tag key-value pairs in the request for DataMigration	String
dms:data-provider-tag/${TagKey}	Filters access by the presence of tag key-value pairs in the request for DataProvider	String
dms:endpoint-tag/${TagKey}	Filters access by the presence of tag key-value pairs in the request for Endpoint	String
dms:es-tag/${TagKey}	Filters access by the presence of tag key-value pairs in the request for EventSubscription	String
dms:individual-assessment-tag/${TagKey}	Filters access by the presence of tag key-value pairs in the request for IndividualAssessment	String
dms:instance-profile-tag/${TagKey}	Filters access by the presence of tag key-value pairs in the request for InstanceProfile	String
dms:migration-project-tag/${TagKey}	Filters access by the presence of tag key-value pairs in the request for MigrationProject	String
dms:rep-tag/${TagKey}	Filters access by the presence of tag key-value pairs in the request for ReplicationInstance	String
dms:replication-config-tag/${TagKey}	Filters access by the presence of tag key-value pairs in the request for ReplicationConfig	String
dms:req-tag/${TagKey}	Filters access by the presence of tag key-value pairs in the given request	String

Condition keys	Description	Type
dms:subgrp-tag/${TagKey}	Filters access by the presence of tag key-value pairs in the request for ReplicationSubnetGroup	String
dms:task-tag/${TagKey}	Filters access by the presence of tag key-value pairs in the request for ReplicationTask	String

Actions, resources, and condition keys for Amazon Direct Connect

Amazon Direct Connect (service prefix: `directconnect`) 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 Direct Connect
- Resource types defined by Amazon Direct Connect
- Condition keys for Amazon Direct Connect

Actions defined by Amazon Direct Connect

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 Amazon. 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.

> **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
AcceptDirectConnectGatewayAssociationProposal	Grants permission to accept a proposal request to attach a virtual private gateway to a Direct Connect gateway	Write	dx-gateway*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AllocateConnectionOnInterconnect	Grants permission to create a hosted connection on an interconnect	Write	dxcon*		
AllocateHostedConnection	Grants permission to create a new hosted connection between a Amazon Direct Connect partner's network and a specific Amazon Direct Connect location	Write	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
AllocatePrivateVirtualInterface	Grants permission to provision a private virtual interface to be owned by a different customer	Write	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
AllocatePublicVirtualInterface	Grants permission to provision a public virtual interface to be owned by a different customer	Write	dxcon		
			dxlag		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
AllocateTransitVirtualInterface	Grants permission to provision a transit virtual interface to be owned by a different customer	Write	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
AssociateConnectionWithLag	Grants permission to associate a connection with a LAG	Write	dxcon*		
			dxlag*		
AssociateHostedConnection	Grants permission to associate a hosted connection and its virtual interfaces with a link aggregation group (LAG) or interconnect	Write	dxcon*		
			dxcon		
			dxlag		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateMacSecKey	Grants permission to associate a MAC Security (MACsec) Connection Key Name (CKN)/ Connectivity Association Key (CAK) pair with an Amazon Direct Connect dedicated connection	Write	dxcon		
			dxlag		
AssociateVirtualInterface	Grants permission to associate a virtual interface with a specified link aggregation group (LAG) or connection	Write	dxvif*		
			dxcon		
			dxlag		
ConfirmConnection	Grants permission to confirm the creation of a hosted connection on an interconnect	Write	dxcon*		
ConfirmCustomerAgreement	Grants permission to confirm the the terms of agreement when creating the connection or link aggregation group (LAG)	Write			
ConfirmPrivateVirtualInterface	Grants permission to accept ownership of a private virtual interface created by another customer	Write	dxvif*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ConfirmPublicVirtualInterface	Grants permission to accept ownership of a public virtual interface created by another customer	Write	dxvif*		
ConfirmTransitVirtualInterface	Grants permission to accept ownership of a transit virtual interface created by another customer	Write	dxvif*		
CreateBGPPeer	Grants permission to create a BGP peer on the specified virtual interface	Write	dxvif*		
CreateConnection	Grants permission to create a new connection between the customer network and a specific Amazon Direct Connect location	Write	dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDirectConnectGateway	Grants permission to create a Direct Connect gateway, which is an intermediate object that enables you to connect a set of virtual interfaces and virtual private gateways	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDirectConnectGatewayAssociation	Grants permission to create an association between a Direct Connect gateway and a virtual private gateway	Write	dx-gateway*		
CreateDirectConnectGatewayAssociationProposal	Grants permission to create a proposal to associate the specified virtual private gateway with the specified Direct Connect gateway	Write	dx-gateway*		
CreateInterconnect	Grants permission to create a new interconnect between a Amazon Direct Connect partner's network and a specific Amazon Direct Connect location	Write	dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateLag	Grants permission to create a link aggregation group (LAG) with the specified number of bundled physical connections between the customer network and a specific Amazon Direct Connect location	Write	dxcon		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePrivateVirtualInterface	Grants permission to create a new private virtual interface	Write	dxcon		
			dxlag		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePublicVirtualInterface	Grants permission to create a new public virtual interface	Write	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTransitVirtualInterface	Grants permission to create a new transit virtual interface	Write	dxcon		
			dxlag		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteBGPPeer	Grants permission to delete the specified BGP peer on the specified virtual interface with the specified customer address and ASN	Write	dxvif*		
DeleteConnection	Grants permission to delete the connection	Write	dxcon*		
DeleteDirectConnectGateway	Grants permission to delete the specified Direct Connect gateway	Write	dx-gateway*		
DeleteDirectConnectGatewayAssociation	Grants permission to delete the association between the specified Direct Connect gateway and virtual private gateway	Write	dx-gateway*		
DeleteDirectConnectGatewayAssociationProposal	Grants permission to delete the association proposal request between the specified Direct Connect gateway and virtual private gateway	Write			
DeleteInterconnect	Grants permission to delete the specified interconnect	Write	dxcon*		
DeleteLag	Grants permission to delete the specified link aggregation group (LAG)	Write	dxlag*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVirtualInterface	Grants permission to delete a virtual interface	Write	dxvif*		
DescribeConnectionLoa	Grants permission to describe the LOA-CFA for a Connection	Read	dxcon*		
DescribeConnections	Grants permission to describe all connections in this region	Read	dxcon		
DescribeConnectionsOnInterconnect	Grants permission to describe a list of connections that have been provisioned on the given interconnect	Read	dxcon*		
DescribeCustomerMetadata	Grants permission to view a list of customer agreements, along with their signed status and whether the customer is an NNIPartner, NNIPartnerV2, or a nonPartner	Read			
DescribeDirectConnectGatewayAssociationProposals	Grants permission to describe one or more association proposals for connection between a virtual private gateway and a Direct Connect gateway	Read	dx-gateway		
DescribeDirectConnectGatewayAssociations	Grants permission to describe the associations between your Direct Connect gateways and virtual private gateways	Read	dx-gateway		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDirectConnectGatewayAttachments	Grants permission to describe the attachments between your Direct Connect gateways and virtual interfaces	Read	dx-gateway		
DescribeDirectConnectGateways	Grants permission to describe all your Direct Connect gateways or only the specified Direct Connect gateway	Read	dx-gateway		
DescribeHostedConnections	Grants permission to describe the hosted connections that have been provisioned on the specified interconnect or link aggregation group (LAG)	Read	dxcon		
			dxlag		
DescribeInterconnectLoa	Grants permission to describe the LOA-CFA for an Interconnect	Read	dxcon*		
DescribeInterconnects	Grants permission to describe a list of interconnects owned by the Amazon Web Services account	Read	dxcon		
DescribeLags	Grants permission to describe all your link aggregation groups (LAG) or the specified LAG	Read	dxlag		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeLoa	Grants permission to describe the LOA-CFA for a connection, interconnect, or link aggregation group (LAG)	Read	dxcon		
			dxlag		
DescribeLocations	Grants permission to describe the list of Amazon Direct Connect locations in the current Amazon region	Read			
DescribeRouterConfiguration	Grants permission to describe Details about the router for a virtual interface	Read	dxvif*		
DescribeTags	Grants permission to describe the tags associated with the specified Amazon Direct Connect resources	Read	dx-gateway		
			dxcon		
			dxlag		
			dxvif		
DescribeVirtualGateways	Grants permission to describe a list of virtual private gateways owned by the Amazon Web Services account	Read			
DescribeVirtualInterfaces	Grants permission to describe all virtual interfaces for an Amazon Web Services account	Read	dxcon		
			dxlag		
			dxvif		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateConnectionFromLag	Grants permission to disassociate a connection from a link aggregation group (LAG)	Write	dxcon*		
			dxlag*		
DisassociateMacSecKey	Grants permission to remove the association between a MAC Security (MACsec) security key and an Amazon Direct Connect dedicated connection	Write	dxcon		
			dxlag		
ListVirtualInterfaceTestHistory	Grants permission to list the virtual interface failover test history	List	dxvif*		
StartBgpFailoverTest	Grants permission to start the virtual interface failover test that verifies your configuration meets your resiliency requirements by placing the BGP peering session in the DOWN state. You can then send traffic to verify that there are no outages	Write	dxvif*		
StopBgpFailoverTest	Grants permission to stop the virtual interface failover test	Write	dxvif*		
TagResource	Grants permission to add the specified tags to the specified Amazon Direct Connect resource. Each resource can have a maximum of 50 tags	Tagging	dx-gateway		
			dxcon		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			dxlag		
			dxvif		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove one or more tags from the specified Amazon Direct Connect resource	Tagging	dx-gateway		
			dxcon		
			dxlag		
			dxvif		
				aws:TagKeys	
UpdateConnection	Grants permission to update the Amazon Direct Connect dedicated connection configuration. You can update the following parameters for a connection: The connection name or The connection's MAC Security (MACsec) encryption mode	Write	dxcon*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateDirectConnectGateway	Grants permission to update the name of a Direct Connect gateway	Write	dx-gateway*		
UpdateDirectConnectGatewayAssociation	Grants permission to update the specified attributes of the Direct Connect gateway association	Write			
UpdateLag	Grants permission to update the attributes of the specified link aggregation group (LAG)	Write	dxlag*		
UpdateVirtualInterfaceAttributes	Grants permission to update the specified attributes of the specified virtual private interface	Write	dxvif*		

Resource types defined by Amazon Direct Connect

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
dxcon	`arn:${Partition}:directconnect:${Region}:${Account}:dxcon/${ConnectionId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
dxlag	`arn:${Partition}:directconnect:${Region}:${Account}:dxlag/${LagId}`	aws:ResourceTag/${TagKey}
dxvif	`arn:${Partition}:directconnect:${Region}:${Account}:dxvif/${VirtualInterfaceId}`	aws:ResourceTag/${TagKey}
dx-gateway	`arn:${Partition}:directconnect::${Account}:dx-gateway/${DirectConnectGatewayId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Direct Connect

Amazon Direct Connect 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 Amazon 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
aws:TagKeys	Filters access by actions based on the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Directory Service

Amazon Directory Service (service prefix: `ds`) 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 Directory Service
- Resource types defined by Amazon Directory Service
- Condition keys for Amazon Directory Service

Actions defined by Amazon Directory 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 Amazon. 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.

> **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
AcceptSharedDirectory	Grants permission to accept a directory sharing request that was sent from the directory owner account	Write	directory*		
AccessDSData [permission only]	Grants permission to access directory data using the Directory Service Data API	Permissions management	directory*		
AddIpRoutes	Grants permission to add a CIDR address block to correctly route traffic to and from your Microsoft AD on Amazon Web Services	Write	directory*		ec2:AuthorizeSecurityGroupEgress

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddRegion	Grants permission to add two domain controllers in the specified Region for the specified directory	Write	directory*		ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddTagsToResource	Grants permission to add or overwrite one or more tags for the specified Amazon Directory Services directory	Tagging	directory*		ec2:CreateTags
				aws:RequestTag/${TagKey} aws:TagKeys	
AuthorizeApplication [permission only]	Grants permission to authorize an application for your Amazon Directory	Write	directory*		
CancelSchemaExtension	Grants permission to cancel an in-progress schema extension to a Microsoft AD directory	Write	directory*		
CheckAlias [permission only]	Grants permission to verify that the alias is available for use	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ConnectDirectory	Grants permission to create an AD Connector to connect to an on-premises directory	Write		aws:RequestTag/${TagKey} aws:TagKeys	ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAlias	Grants permission to create an alias for a directory and assigns the alias to the directory	Write	directory*		
CreateComputer	Grants permission to create a computer account in the specified directory, and joins the computer to the directory	Write	directory*		
CreateConditionalForwarder	Grants permission to create a conditional forwarder associated with your Amazon directory	Write	directory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDirectory	Grants permission to create a Simple AD directory	Write		aws:RequestTag/${TagKey} aws:TagKeys	ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateIdentityPoolDirectory [permission only]	Grants permission to create an IdentityPool Directory in the Amazon cloud	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLogSubscription	Grants permission to create a subscription to forward real time Directory Service domain controller security logs to the specified CloudWatch log group in your Amazon Web Services account	Write	directory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateMicrosoftAD	Grants permission to create a Microsoft AD in the Amazon cloud	Write		aws:RequestTag/${TagKey} aws:TagKeys	ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateNetworkInterface ec2:CreateSecurityGroup ec2:CreateTags ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSnapshot	Grants permission to create a snapshot of a Simple AD or Microsoft AD directory in the Amazon cloud	Write	directory*		
CreateTrust	Grants permission to initiate the creation of the Amazon side of a trust relationship between a Microsoft AD in the Amazon cloud and an external domain	Write	directory*		
DeleteConditionalForwarder	Grants permission to delete a conditional forwarder that has been set up for your Amazon directory	Write	directory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteDirectory	Grants permission to delete an Amazon Directory Service directory	Write	directory*		ec2:DeleteNetworkInterface ec2:DeleteSecurityGroup ec2:DescribeNetworkInterfaces ec2:RevokeSecurityGroupEgress ec2:RevokeSecurityGroupIngress
DeleteLogSubscription	Grants permission to delete the specified log subscription	Write	directory*		
DeleteSnapshot	Grants permission to delete a directory snapshot	Write	directory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTrust	Grants permission to delete an existing trust relationship between your Microsoft AD in the Amazon cloud and an external domain	Write	directory*		
DeregisterCertificate	Grants permission to delete from the system the certificate that was registered for a secured LDAP connection	Write	directory*		
DeregisterEventTopic	Grants permission to remove the specified directory as a publisher to the specified SNS topic	Write	directory*		
DescribeCertificate	Grants permission to display information about the certificate registered for a secured LDAP connection	Read	directory*		
DescribeClientAuthenticationSettings	Grants permission to retrieve information about the type of client authentication for the specified directory, if the type is specified. If no type is specified, information about all client authentication types that are supported for the specified directory is retrieved. Currently, only SmartCard is supported	Read	directory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeConditionalForwarders	Grants permission to obtain information about the conditional forwarders for this account	Read	directory*		
DescribeDirectories	Grants permission to obtain information about the directories that belong to this account	List			
DescribeDirectoryDataAccess	Grants permission to describe the Directory Service Data API status for the specified directory	Read	directory*		
DescribeDomainControllers	Grants permission to provide information about any domain controllers in your directory	Read	directory*		
DescribeEventTopics	Grants permission to obtain information about which SNS topics receive status messages from the specified directory	Read	directory*		
DescribeLDAPSSettings	Grants permission to describe the status of LDAP security for the specified directory	Read	directory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeRegions	Grants permission to provide information about the Regions that are configured for multi-Region replication	Read	directory*		
DescribeSettings	Grants permission to retrieve information about the configurable settings for the specified directory	Read	directory*		
DescribeSharedDirectories	Grants permission to return the shared directories in your account	Read	directory*		
DescribeSnapshots	Grants permission to obtain information about the directory snapshots that belong to this account	Read			
DescribeTrusts	Grants permission to obtain information about the trust relationships for this account	Read			
DescribeUpdateDirectory	Grants permission to describe the updates of a directory for a particular update type	Read	directory*		
DisableClientAuthentication	Grants permission to disable alternative client authentication methods for the specified directory	Write	directory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableDirectoryDataAccess	Grants permission to disable the Directory Service Data API for the specified directory	Write	directory*		
DisableLDAPS	Grants permission to deactivate LDAP secure calls for the specified directory	Write	directory*		
DisableRadius	Grants permission to disable multi-factor authentication (MFA) with the Remote Authentication Dial In User Service (RADIUS) server for an AD Connector directory	Write	directory*		
DisableRoleAccess [permission only]	Grants permission to disable Amazon Web Services Management Console access for identity in your Amazon Directory	Write	directory*		
DisableSso	Grants permission to disable single-sign on for a directory	Write	directory*		
EnableClientAuthentication	Grants permission to enable alternative client authentication methods for the specified directory	Write	directory*		
EnableDirectoryDataAccess	Grants permission to enable the Directory Service Data API for the specified directory	Write	directory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableLDAPS	Grants permission to activate the switch for the specific directory to always use LDAP secure calls	Write	directory*		
EnableRadius	Grants permission to enable multi-factor authentication (MFA) with the Remote Authentication Dial In User Service (RADIUS) server for an AD Connector directory	Write	directory*		
EnableRoleAccess [permission only]	Grants permission to enable Amazon Web Services Management Console access for identity in your Amazon Directory	Write	directory*		iam:PassRole
EnableSso	Grants permission to enable single-sign on for a directory	Write	directory*		
GetAuthorizedApplicationDetails [permission only]	Grants permission to retrieve the details of the authorized applications on a directory	Read	directory*		
GetDirectoryLimits	Grants permission to obtain directory limit information for the current region	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSnapshotLimits	Grants permission to obtain the manual snapshot limits for a directory	Read	directory*		
ListAuthorizedApplications [permission only]	Grants permission to obtain the Amazon applications authorized for a directory	Read	directory*		
ListCertificates	Grants permission to list all the certificates registered for a secured LDAP connection, for the specified directory	List	directory*		
ListIpRoutes	Grants permission to list the address blocks that you have added to a directory	Read	directory*		
ListLogSubscriptions	Grants permission to list the active log subscriptions for the Amazon Web Services account	Read			
ListSchemaExtensions	Grants permission to list all schema extensions applied to a Microsoft AD Directory	List	directory*		
ListTagsForResource	Grants permission to list all tags on an Amazon Directory Services directory	Read	directory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterCertificate	Grants permission to register a certificate for secured LDAP connection	Write	directory*		
RegisterEventTopic	Grants permission to associate a directory with an SNS topic	Write	directory*		sns:GetTopicAttributes
RejectSharedDirectory	Grants permission to reject a directory sharing request that was sent from the directory owner account	Write	directory*		
RemoveIpRoutes	Grants permission to remove IP address blocks from a directory	Write	directory*		
RemoveRegion	Grants permission to stop all replication and removes the domain controllers from the specified Region. You cannot remove the primary Region with this operation	Write	directory*		
RemoveTagsFromResource	Grants permission to remove tags from an Amazon Directory Services directory	Tagging	directory*		ec2:DeleteTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
ResetUserPassword	Grants permission to reset the password for any user in your Amazon Managed Microsoft AD or Simple AD directory	Write	directory*		
RestoreFromSnapshot	Grants permission to restore a directory using an existing directory snapshot	Write	directory*		
ShareDirectory	Grants permission to share a specified directory in your Amazon Web Services account (directory owner) with another Amazon Web Services account (director y consumer). With this operation you can use your directory from any Amazon Web Services account and from any Amazon VPC within an Amazon Web Services Region	Write	directory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartSchemaExtension	Grants permission to apply a schema extension to a Microsoft AD directory	Write	directory*		
UnauthorizeApplication [permission only]	Grants permission to unauthorize an application from your Amazon Directory	Write	directory*		
UnshareDirectory	Grants permission to stop the directory sharing between the directory owner and consumer accounts	Write	directory*		
UpdateAuthorizedApplication [permission only]	Grants permission to update an authorized application for your Amazon Directory	Write	directory*		
UpdateConditionalForwarder	Grants permission to update a conditional forwarder that has been set up for your Amazon directory	Write	directory*		
UpdateDirectory [permission only]	Grants permission to update the configurations like service account credentials or DNS server IP addresses for the specified directory	Write	directory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateDirectorySetup	Grants permission to update the directory for a particular update type	Write	directory*		
UpdateNumberOfDomainControllers	Grants permission to add or remove domain controllers to or from the directory. Based on the difference between current value and new value (provided through this API call), domain controllers will be added or removed. It may take up to 45 minutes for any new domain controllers to become fully active once the requested number of domain controllers is updated. During this time, you cannot make another update request	Write	directory*		
UpdateRadius	Grants permission to update the Remote Authentication Dial In User Service (RADIUS) server information for an AD Connector directory	Write	directory*		
UpdateSettings	Grants permission to update the configurable settings for the specified directory	Write	directory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateTrust	Grants permission to update the trust that has been set up between your Amazon Managed Microsoft AD directory and an on-premises Active Directory	Write	directory*		
VerifyTrust	Grants permission to verify a trust relationship between your Microsoft AD in the Amazon cloud and an external domain	Read	directory*		

Resource types defined by Amazon Directory 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
directory	`arn:${Partition}:ds:${Region}:${Account}:directory/${DirectoryId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Directory Service

Amazon Directory 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 Amazon global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the value of the request to Amazon DS	String
aws:ResourceTag/${TagKey}	Filters access by the Amazon DS Resource being acted upon	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString

Actions, resources, and condition keys for Amazon DynamoDB

Amazon DynamoDB (service prefix: `dynamodb`) 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 DynamoDB
- Resource types defined by Amazon DynamoDB
- Condition keys for Amazon DynamoDB

Actions defined by Amazon DynamoDB

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 Amazon. 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.

> **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
BatchGetItem	Grants permission to return the attributes of one or more items from one or more tables	Read	table*		
				dynamodb:Attributes dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:Select	
BatchWriteItem	Grants permission to put or delete multiple items in one or more tables	Write	table*		
				dynamodb:Attributes dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ConditionCheckItem	Grants permission to the ConditionCheckItem operation checks the existence of a set of attributes for the item with the given primary key	Read	table*		
				dynamodb:Attributes dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues	
CreateBackup	Grants permission to create a backup for an existing table	Write	table*		
CreateGlobalTable	Grants permission to create a global table from an existing table	Write	global-table*		
			table*		
CreateTable	Grants permission to the CreateTable operation adds a new table to your account	Write	table*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTableReplica [permission only]	Grants permission to add a new replica table	Write	table*		
DeleteBackup	Grants permission to delete an existing backup of a table	Write	backup*		
DeleteItem	Grants permission to deletes a single item in a table by primary key	Write	table*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues	
DeleteResourcePolicy	Grants permission to delete the resource-based policy attached to the resource	Permissions management	stream* table*		
DeleteTable	Grants permission to the DeleteTable operation which deletes a table and all of its items	Write	table*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTableReplica [permission only]	Grants permission to delete a replica table and all of its items	Write	table*		
DescribeBackup	Grants permission to describe an existing backup of a table	Read	backup*		
DescribeContinuousBackups	Grants permission to check the status of the backup restore settings on the specified table	Read	table*		
DescribeContributorInsights	Grants permission to describe the contributor insights status and related details for a given table or global secondary index	Read	table* index		
DescribeEndpoints	Grants permission to return the regional endpoint information	Read			
DescribeExport	Grants permission to describe an existing Export of a table	Read	export*		
DescribeGlobalTable	Grants permission to return information about the specified global table	Read	global-table*		
DescribeGlobalTableSettings	Grants permission to return settings information about the specified global table	Read	global-table*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeImport	Grants permission to describe an existing import	Read	import*		
DescribeKinesisStreamingDestination	Grants permission to grant permission to describe the status of Kinesis streaming and related details for a given table	Read	table*		
DescribeLimits	Grants permission to return the current provisioned-capacity limits for your Amazon Web Services account in a region, both for the region as a whole and for any one DynamoDB table that you create there	Read			
DescribeReservedCapacity [permission only]	Grants permission to describe one or more of the Reserved Capacity purchased	Read			
DescribeReservedCapacityOfferings [permission only]	Grants permission to describe Reserved Capacity offerings that are available for purchase	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeStream	Grants permission to return information about a stream, including the current status of the stream, its Amazon Resource Name (ARN), the composition of its shards, and its corresponding DynamoDB table	Read	stream*		
DescribeTable	Grants permission to return information about the table	Read	table*		
DescribeTableReplicaAutoScaling	Grants permission to describe the auto scaling settings across all replicas of the global table	Read	table*		
DescribeTimeToLive	Grants permission to give a description of the Time to Live (TTL) status on the specified table	Read	table*		
DisableKinesisStreamingDestination	Grants permission to grant permission to stop replication from the DynamoDB table to the Kinesis data stream	Write	table*		
EnableKinesisStreamingDestination	Grants permission to grant permission to start table data replication to the specified Kinesis data stream at a timestamp chosen during the enable workflow	Write	table*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ExportTableToPointInTime	Grants permission to initiate an Export of a DynamoDB table to S3	Write	table*		
GetAbacStatus [permission only]	Grants permission to view the status of Attribute Based Access Control for the account	Read			
GetItem	Grants permission to the GetItem operation that returns a set of attributes for the item with the given primary key	Read	table*		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:Select	
GetRecords	Grants permission to retrieve the stream records from a given shard	Read	stream*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetResourcePolicy	Grants permission to view a resource-based policy for a resource	Read	stream*		
			table*		
GetShardIterator	Grants permission to return a shard iterator	Read	stream*		
ImportTable	Grants permission to initiate an import from S3 to a DynamoDB table	Write	table*		
ListBackups	Grants permission to list backups associated with the account and endpoint	List			
ListContributorInsights	Grants permission to list the ContributorInsightsSummary for all tables and global secondary indexes associated with the current account and endpoint	List			
ListExports	Grants permission to list exports associated with the account and endpoint	List			
ListGlobalTables	Grants permission to list all global tables that have a replica in the specified region	List			
ListImports	Grants permission to list imports associated with the account and endpoint	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListStreams	Grants permission to return an array of stream ARNs associated with the current account and endpoint	Read			
ListTables	Grants permission to return an array of table names associated with the current account and endpoint	List			
ListTagsOfResource	Grants permission to list all tags on an Amazon DynamoDB resource	Read	table*		
PartiQLDelete	Grants permission to delete a single item in a table by primary key	Write	table*		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnValues	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PartiQLInsert	Grants permission to create a new item, if an item with same primary key does not exist in the table	Write	table*		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys	
PartiQLSelect	Grants permission to read a set of attributes for items from a table or index	Read	table*		
			index		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:FullTableScan dynamodb:LeadingKeys dynamodb:Select	
PartiQLUpdate	Grants permission to edit an existing item's attributes	Write	table*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnValues	
PurchaseReservedCapacityOfferings [permission only]	Grants permission to purchases reserved capacity for use with your account	Write			
PutItem	Grants permission to create a new item, or replace an old item with a new item	Write	table*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues	
PutResourcePolicy	Grants permission to attach a resource-based policy to the resource	Permissions management	stream* table*		
Query	Grants permission to use the primary key of a table or a secondary index to directly access items from that table or index	Read	table* index		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				dynamodb:Attributes dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues dynamodb:Select	
RestoreTableFromAwsBackup [permission only]	Grants permission to create a new table from recovery point on Amazon Backup	Write	table*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RestoreTableFromBackup	Grants permission to create a new table from an existing backup	Write	backup*		dynamodb:BatchWriteItem dynamodb:DeleteItem dynamodb:GetItem dynamodb:PutItem dynamodb:Query dynamodb:Scan dynamodb:UpdateItem
			table*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RestoreTableToPointInTime	Grants permission to restore a table to a point in time	Write	table*		dynamodb:BatchWriteItem dynamodb:DeleteItem dynamodb:GetItem dynamodb:PutItem dynamodb:Query dynamodb:Scan dynamodb:UpdateItem
Scan	Grants permission to return one or more items and item attributes by accessing every item in a table or a secondary index	Read	table*		
			index		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				dynamodb:Attributes dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues dynamodb:Select	
StartAwsBackupJob [permission only]	Grants permission to create a backup on Amazon Backup with advanced features enabled	Write	table*		
TagResource	Grants permission to associate a set of tags with an Amazon DynamoDB resource	Tagging	table*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagResource	Grants permission to remove the association of tags from an Amazon DynamoDB resource	Tagging	table*		
				aws:TagKeys	
UpdateAbacStatus [permission only]	Grants permission to update the status of Attribute Based Access Control for the account	Permissions management			
UpdateContinuousBackups	Grants permission to enable or disable continuous backups	Write	table*		
UpdateContributorInsights	Grants permission to update the status for contributor insights for a specific table or global secondary index	Write	table*		
			index		
UpdateGlobalTable	Grants permission to add or remove replicas in the specified global table	Write	global-table*		
			table*		
UpdateGlobalTableSettings	Grants permission to update settings of the specified global table	Write	global-table*		
			table*		
UpdateGlobalTableVersion [permission only]	Grants permission to update version of the specified global table	Write	global-table*		
			table		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateItem	Grants permission to edit an existing item's attributes, or adds a new item to the table if it does not already exist	Write	table*		
				dynamodb:Attributes dynamodb:EnclosingOperation dynamodb:LeadingKeys dynamodb:ReturnConsumedCapacity dynamodb:ReturnValues	
UpdateKinesisStreamingDestination	Grants permission to update data replication configurations for the specified Kinesis data stream	Write	table*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateTable	Grants permission to modify the provisioned throughput settings, global secondary indexes, or DynamoDB Streams settings for a given table	Write	table*		
UpdateTableReplicaAutoScaling	Grants permission to update auto scaling settings on your replica table	Write	table*		
UpdateTimeToLive	Grants permission to enable or disable TTL for the specified table	Write	table*		

Resource types defined by Amazon DynamoDB

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
index	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/index/${IndexName}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
stream	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/stream/${StreamLabel}`	
table	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}`	aws:ResourceTag/${TagKey}
backup	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/backup/${BackupName}`	
export	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/export/${ExportName}`	
global-table	`arn:${Partition}:dynamodb::${Account}:global-table/${GlobalTableName}`	
import	`arn:${Partition}:dynamodb:${Region}:${Account}:table/${TableName}/import/${ImportName}`	

Condition keys for Amazon DynamoDB

Amazon DynamoDB 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 Amazon global condition context keys.

> **Note**
>
> For information about how to use context keys to refine DynamoDB access using an IAM policy, see Using IAM Policy Conditions for Fine-Grained Access Control in the *Amazon DynamoDB Developer Guide*.

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
dynamodb:Attributes	Filters access by attribute (field or column) names of the table	ArrayOfString
dynamodb:EnclosingOperation	Filters access by blocking Transactions APIs calls and allow the non-Transaction APIs calls and vice-versa	String
dynamodb:FullTableScan	Filters access by blocking full table scan	Bool
dynamodb:LeadingKeys	Filters access by the partition key of the table	ArrayOfString
dynamodb:ReturnConsumedCapacity	Filters access by the ReturnConsumedCapacity parameter of a request. Contains either "TOTAL" or "NONE"	String

Condition keys	Description	Type
dynamodb: ReturnValues	Filters access by the ReturnValues parameter of request. Contains one of the following: "ALL_OLD", "UPDATED_OLD","ALL_NEW","UPDATED_NEW", or "NONE"	String
dynamodb: Select	Filters access by the Select parameter of a Query or Scan request	String

Actions, resources, and condition keys for Amazon DynamoDB Accelerator (DAX)

Amazon DynamoDB Accelerator (DAX) (service prefix: `dax`) 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 DynamoDB Accelerator (DAX)
- Resource types defined by Amazon DynamoDB Accelerator (DAX)
- Condition keys for Amazon DynamoDB Accelerator (DAX)

Actions defined by Amazon DynamoDB Accelerator (DAX)

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 Amazon. 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.

> **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
BatchGetItem	Grants permission to return the attributes of one or more items from one or more tables	Read	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchWriteItem	Grants permission to put or delete multiple items in one or more tables	Write	application*		
ConditionCheckItem	Grants permission to the ConditionCheckItem operation that checks the existence of a set of attributes for the item with the given primary key	Read	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCluster	Grants permission to create a DAX cluster	Write	application*		dax:CreateParameterGroup dax:CreateSubnetGroup ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs iam:GetRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					iam:PassRole
CreateParameterGroup	Grants permission to create a parameter group	Write			
CreateSubnetGroup	Grants permission to create a subnet group	Write			
DecreaseReplicationFactor	Grants permission to remove one or more nodes from a DAX cluster	Write	application*		
DeleteCluster	Grants permission to delete a previously provisioned DAX cluster	Write	application*		
DeleteItem	Grants permission to delete a single item in a table by primary key	Write	application*		
				dax:EnclosingOperation	
DeleteParameterGroup	Grants permission to delete the specified parameter group	Write			
DeleteSubnetGroup	Grants permission to delete a subnet group	Write			
DescribeClusters	Grants permission to return information about all provisioned DAX clusters	List	application		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDefaultParameters	Grants permission to return the default system parameter information for DAX	List			
DescribeEvents	Grants permission to return events related to DAX clusters and parameter groups	List			
DescribeParameterGroups	Grants permission to return a list of parameter group descriptions	List			
DescribeParameters	Grants permission to return the detailed parameter list for a particular parameter group	Read			
DescribeSubnetGroups	Grants permission to return a list of subnet group descriptions	List			
GetItem	Grants permission to the GetItem operation that returns a set of attributes for the item with the given primary key	Read	application*		
				dax:EnclosingOperation	
IncreaseReplicationFactor	Grants permission to add one or more nodes to a DAX cluster	Write	application*		
ListTags	Grants permission to return a list all of the tags for a DAX cluster	Read	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutItem	Grants permission to create a new item, or replace an old item with a new item	Write	application*		
				dax:EnclosingOperation	
Query	Grants permission to use the primary key of a table or a secondary index to directly access items from that table or index	Read	application*		
RebootNode	Grants permission to reboot a single node of a DAX cluster	Write	application*		
Scan	Grants permission to return one or more items and item attributes by accessing every item in a table or a secondary index	Read	application*		
TagResource	Grants permission to associate a set of tags with a DAX resource	Tagging	application*		
UntagResource	Grants permission to remove the association of tags from a DAX resource	Tagging	application*		
UpdateCluster	Grants permission to modify the settings for a DAX cluster	Write	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateItem	Grants permission to edit an existing item's attributes, or adds a new item to the table if it does not already exist	Write	application*		
				dax:EnclosingOperation	
UpdateParameterGroup	Grants permission to modify the parameters of a parameter group	Write			
UpdateSubnetGroup	Grants permission to modify an existing subnet group	Write			

Resource types defined by Amazon DynamoDB Accelerator (DAX)

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:${Partition}:dax:${Region}:${Account}:cache/${ClusterName}`	

Condition keys for Amazon DynamoDB Accelerator (DAX)

Amazon DynamoDB Accelerator (DAX) 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 Amazon global condition context keys.

Condition keys	Description	Type
dax:EnclosingOperation	Used to block Transactions APIs calls and allow the non-Transaction APIs calls and vice-versa	String

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 Amazon. 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.

> **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/	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} aws:TagKeys ec2:AllocationId ec2:Domain ec2:PublicIpAddress	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 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
AcceptReservedInstancesExchangeQuote	Grants permission to accept a Convertible Reserved Instance exchange quote	Write		ec2:Region	
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	

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	
AcceptTransitGatewayPeeringAttachment	Grants permission to accept a transit gateway peering attachment request	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	
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	
				ec2:Region	

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

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
			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/${TagKey} ec2:ResourceTag/${TagKey} ec2:SubnetID	
				ec2:Region	
Associate DhcpOptions	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:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType	iam:PassRole

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:NewInstanceProfile ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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}	
				ec2:Region	
AssociateIpamByoasn	Grants permission to associate an Autonomous System Number (ASN) with a BYOIP CIDR	Write		ec2:Region	

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Associate RouteServer	Grants permission to associate a route server with 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	
				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
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
			vpn-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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
Associate SubnetCidrBlock	Grants permission to associate a CIDR block with a subnet	Write	subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
			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/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
			transit-gateway-attachment*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayAttachmentId	

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	
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	

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

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	
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 Amazon Web Application Firewall (WAF) web access control list (ACL) with a Verified Access instance	Write	verified-access-instance*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

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

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: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:PlacementGroup ec2:ResourceTag/	

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

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
			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: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:PlacementGroup ec2:ProductCode	

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
			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	
				ec2:Region	
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}	

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Authorize ClientVpn Ingress	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 Amazon Web Services account from the launch permissions for 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
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:SnapshotID ec2:SnapshotTime ec2:VolumeSize	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/${TagKey} ec2:ResourceTag/${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/${TagKey}	
				ec2:Region	
CreateCoipPoolPermission [permission only]	Grants permission to allow a service to access a customer-owned IP (CoIP) pool	Write	coip-pool*	aws:ResourceTag/${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 Amazon about your customer gateway device	Write	customer-gateway*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	
CreateDefaultSubnet	Grants permission to create a default subnet in a specified Availability Zone in a default VPC	Write		ec2:Region	
CreateDefaultVpc	Grants permission to create a default VPC with a default subnet in each Availability Zone	Write		ec2:Region	
CreateDhcpOptions	Grants permission to create a set of DHCP options for a VPC	Write	dhcp-options*	aws:RequestTag/${TagKey} aws:TagKeys ec2:DhcpOptionsID	ec2:CreateTags
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateEgressOnlyInternetGateway	Grants permission to create an egress-only internet gateway for a VPC	Write	egress-only-internet-gateway*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
			vpc*	aws:ResourceTag/${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 permissio ns 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:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceBandwidthWeighting ec2:InstanceID	

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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
			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/${TagKey} aws:TagKeys ec2:Owner ec2:Public	ec2:CreateTags
				ec2:Region	
CreateImage	Grants permission to create an Amazon EBS-backed AMI from a stopped or running Amazon EBS-backed instance	Write	image*	aws:RequestTag/${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: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:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey}	

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Tenancy	
				ec2:Region	
CreateInternetGateway	Grants permission to create an internet gateway for a VPC	Write	internet-gateway*	aws:RequestTag/${TagKey} aws:TagKeys ec2:InternetGatewayID	ec2:CreateTags
				ec2:Region	
CreateIpam	Grants permission to create an Amazon VPC IP Address Manager (IPAM)	Write	ipam*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags iam:CreateServiceLinkedRole
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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/${TagKey} aws:TagKeys	
				ec2:Region	
CreateIpamPool	Grants permission to create an IP address pool for Amazon VPC IP Address Manager (IPAM), which is a collection of contiguous IP address CIDRs	Write	ipam-pool*	aws:RequestTag/${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	
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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
CreateLaunchTemplateVersion	Grants permission to create a new version of a launch template	Write	launch-template*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${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	Write	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/${TagKey} aws:TagKeys	
				ec2:Region	
CreateManagedPrefixList	Grants permission to create a managed prefix list	Write	prefix-list*	aws:RequestTag/${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
			subnet*	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

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}	
				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: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:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup ec2:ProductCode ec2:ResourceTag/${TagKey}	

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
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:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType	ec2:CreateTags

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

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

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:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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/${TagKey} aws:TagKeys ec2:SubnetID	ec2:CreateTags
			vpc*	aws:ResourceTag/${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	
CreateSubnetCidrReservation	Grants permission to create a subnet CIDR reservation	Write		ec2:Region	
CreateTags	Grants permission to add or overwrite one or more tags for Amazon EC2 resources	Tagging	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
			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: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:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit ec2:MetadataHttpTokens ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ProductCode ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
			instance-connect-endpoint	aws:RequestTag/${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-pool	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: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:NetworkInterfaceID ec2:Permission ec2:ResourceTag/${TagKey} ec2:Subnet	

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			traffic-mirror-session*	aws:RequestTag/${TagKey} aws:TagKeys	
			traffic-mirror-target*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
CreateTrafficMirrorTarget	Grants permission to create a traffic mirror target	Write	traffic-mirror-target*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			network-interface	aws:ResourceTag/${TagKey} ec2:NetworkInterfaceID ec2:ResourceTag/${TagKey}	
			vpc-endpoint	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:VpceServiceName ec2:VpceServiceOwner	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
CreateTransitGateway	Grants permission to create a transit gateway	Write	transit-gateway*	aws:RequestTag/${TagKey} aws:TagKeys ec2:transitGatewayId	ec2:CreateTags
				ec2:Region	
CreateTransitGatewayConnect	Grants permission to create a Connect attachment from a specified transit gateway attachment	Write	transit-gateway-attachment*	aws:RequestTag/${TagKey} aws:TagKeys ec2:transitGatewayAttachmentId	ec2:CreateTags
				ec2:Region	

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
CreateVerifiedAccessGroup	Grants permission to create a Verified Access group	Write	verified-access-group*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags
			verified-access-instance*	aws:ResourceTag/${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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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:Encrypted ec2:KmsKeyId ec2:ParentSnapshot ec2:VolumeID ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput	ec2:CreateTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeType	
			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/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${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
CreateVpcEndpoint	Grants permission to create a VPC endpoint for an Amazon service	Write	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:VpcID	ec2:CreateTags route53:AssociateVPCWithHostedZone
			vpc-endpoint*	aws:RequestTag/${TagKey} aws:TagKeys ec2:VpceServiceName ec2:VpceServiceOwner	

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 (Amazon accounts, IAM users, and IAM roles) can connect	Write	vpc-endpoint-service*	aws:RequestTag/${TagKey} aws:TagKeys ec2:VpceServicePrivateDnsName ec2:vpceMultiRegion 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	
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-gateway	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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/${TagKey} aws:TagKeys	ec2:CreateTags
				ec2:Region	
DeleteCarrierGateway	Grants permission to delete a carrier gateway	Write	carrier-gateway*	aws:ResourceTag/${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
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/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	
DeleteCoipCidr	Grants permission to delete 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
DeleteCoipPool	Grants permission to delete a pool of customer-owned IP (CoIP) addresses	Write	coip-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteCoipPoolPermission [permission only]	Grants permission to deny a service from accessing a customer-owned IP (CoIP) pool	Write	coip-pool*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteCustomerGateway	Grants permission to delete a customer gateway	Write	customer-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteDhcpOptions	Grants permission to delete a set of DHCP options	Write	dhcp-options*	aws:ResourceTag/${TagKey} ec2:DhcpOptionsID ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteEgressOnlyInternetGateway	Grants permission to delete an egress-only internet gateway	Write	egress-only-internet-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteFleets	Grants permission to delete one or more EC2 Fleets	Write	fleet*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteFlowLogs	Grants permission to delete one or more flow logs	Write	vpc-flow-log*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
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	

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	
DeleteIpamPool	Grants permission to delete 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
DeleteIpamResourceDiscovery	Grants permission to delete an IPAM resource discovery	Write	ipam-resource-discovery*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	
DeleteLaunchTemplate	Grants permission to delete a launch template and its associated versions	Write	launch-template*	aws:ResourceTag/${TagKey} ec2:ManagedResourceOperator ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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	
DeleteLocalGatewayRoute	Grants permission to delete a route from 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
			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}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteLocalGatewayRouteTablePermission [permission only]	Grants permission to deny a service from accessing a local gateway route table	Write	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/${TagKey} ec2:ResourceTag/${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
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		ec2:Region	
DeleteResourcePolicy [permission only]	Grants permission to remove an IAM policy that enables cross-account sharing from a resource	Write	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	
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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteRouteServer	Grants permission to delete a route server	Write	route-server*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	sns:DeleteTopic
				ec2:Region	
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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	
DeleteRouteTable	Grants permission to delete a 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
DeleteSecurityGroup	Grants permission to delete 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
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	
				ec2:Region	

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTags	Grants permission to delete one or more tags from Amazon EC2 resources	Tagging	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
			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-pool	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-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-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-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-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
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	
DeleteTransitGatewayPeeringAttachment	Grants permission to delete a peering attachment from 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	
DeleteTransitGatewayPolicyTable	Grants permission to delete a transit gateway policy table	Write	transit-gateway-policy-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayPolicyTableId	
				ec2:Region	
DeleteTransitGatewayPrefixListReference	Grants permission to delete a transit gateway prefix list reference	Write	prefix-list*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

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	
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	

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	
DeleteTransitGatewayVpcAttachment	Grants permission to delete a VPC attachment from 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	
DeleteVerifiedAccessEndpoint	Grants permission to delete a Verified Access endpoint	Write	verified-access-endpoint*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
DeleteVerifiedAccessGroup	Grants permission to delete a Verified Access group	Write	verified-access-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVerifiedAccessInstance	Grants permission to delete a Verified Access instance	Write	verified-access-instance*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
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/${TagKey} ec2:AvailabilityZone ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeIops ec2:VolumeSize	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	
DeleteVpc	Grants permission to delete 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
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	
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:VpceServiceName	
				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	
DeleteVpnConnection	Grants permission to delete a VPN connection	Write	vpn-connection*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 Amazon Web Services 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	
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	
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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 Amazon Web Services 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	
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	

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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	
DescribeInstanceEventWindows	Grants permission to describe the specified event windows or all event windows	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeInstanceImageMetadata	Grants permission to describe the AMI that was used to launch an instance	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	
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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeIpamExternalResourceVerificationTokens	Grants permission to describe verification tokens, which proves ownership of an external resource	List		ec2:Region	
DescribeIpamPools	Grants permission to describe Amazon VPC IP Address Manager (IPAM) pools	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	

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeLocalGatewayRouteTables	Grants permission to describe one or more local gateway route tables	List		ec2:Region	
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	
DescribeManagedPrefixLists	Grants permission to describe your managed prefix lists and any Amazon-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 Amazon 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 Amazon Web Services 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	
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	
DescribeTransitGatewayRouteTables	Grants permission to describe one or more transit gateway route tables	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	
DescribeVerifiedAccessInstanceLoggingConfigurations	Grants permission to describe the current logging configuration for the Verified Access instances	List		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeVerifiedAccessInstanceWebAclAssociations [permission only]	Grants permission to describe the Amazon 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/${TagKey} ec2:AvailabilityZone ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeIops ec2:VolumeSize	

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

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: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:PlacementGroup ec2:ProductCode	

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
			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/${TagKey} ec2:AvailabilityZone ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeIops ec2:VolumeSize	

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

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:PlacementGroup ec2:ProductCode	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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	
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 Amazon Web Services Region	Write		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	
DisableIpamOrganizationAdminAccount	Grants permission to disable an Amazon Organizations member account as an Amazon VPC IP Address Manager (IPAM) admin account	Write		ec2:Region	organizations:DeregisterDelegatedAdministrator

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableRouteServerPropagation	Grants permission to disable route server propagation	Write	route-server*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableSnapshotBlockPublicAccess	Grants permission to disable the block public access for snapshots setting for a Region	Write		ec2:Region	
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	

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
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	
			vpn-gateway*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableVpcClassicLink	Grants permission to disable ClassicLink for a VPC	Write	vpc*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:Tenancy ec2:VpcID	
				ec2:Region	
DisableVpcClassicLinkDnsSupport	Grants permission to disable ClassicLink DNS support for 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	
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: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:PlacementGroup ec2:ProductCode	

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

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

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	
DisassociateTransitGatewayPolicyTable	Grants permission to disassociate a policy table from 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
			transit-gateway-policy-table*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:transitGatewayPolicyTableId	
				ec2:Region	
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	

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	
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 Amazon Web Application Firewall (WAF) web access control list (ACL) from a Verified Access instance	Write	verified-access-instance*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	
EnableAwsNetworkPerformanceMetricSubscription	Grants permission to enable infrastructure performance subscriptions	Write		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 Amazon Web Services Region	Write		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
EnableIpamOrganizationAdminAccount	Grants permission to enable an Amazon Organizations member account as an Amazon VPC IP Address Manager (IPAM) admin account	Write		ec2:Region	iam:CreateServiceLinkedRole organizations:EnableAWSServiceAccess organizations:RegisterDelegatedAdministrator
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}	

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	
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	Write		ec2:Region	

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeThroughput ec2:VolumeType	
				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	
GetAllowedImagesSettings	Grants permission to get the allowed settings for images	Read		ec2:Region	
GetAssociatedEnclaveCertificateIamRoles	Grants permission to get the list of roles associated with an ACM certificate	Read	certificate*		
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAssociatedIpv6PoolCidrs	Grants permission to get information about the IPv6 CIDR block associations for a specified IPv6 address pool	Read		ec2:Region	
GetAwsNetworkPerformanceData	Grants permission to get network performance data	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}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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: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:PlacementGroup 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
GetConsoleScreenshot	Grants permission to retrieve a JPG-format screenshot of a running instance	Read	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:NewInstanceProfile ec2:PlacementGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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}	
				ec2:Region	
GetDefaultCreditSpecification	Grants permission to get the default credit option for CPU usage of a burstable performance instance family	Read		ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	
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}	
				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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
GetHostReservationPurchasePreview	Grants permission to preview a reservation purchase with configurations that match those of a Dedicated Host	Read		ec2:Region	
GetImageBlockPublicAccessState	Grants permission to get the current state of block public access for AMIs at the account level in the specified Amazon Web Services Region	Read		ec2:Region	
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: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	
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: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:NewInstanceProfile ec2:PlacementGroup	

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	
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	
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}	

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
GetReservedInstancesExchangeQuote	Grants permission to return a quote and exchange information for exchanging one or more Convertible Reserved Instances for a new Convertible Reserved Instance	Read		ec2:Region	
GetResourcePolicy [permission only]	Grants permission to describe an IAM policy that enables cross-account sharing	Read	ipam-pool	aws:ResourceTag/${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
GetRouteServerAssociations	Grants permission to get associations for a route server	Read	route-server*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
GetRouteServerPropagations	Grants permission to get propagations for a route server	Read	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	
GetRouteServerRoutingDatabase	Grants permission to get the routing database 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
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	
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	

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetVerifiedAccessEndpointTargets	Grants permission to get verified access endpoint targets	List	verified-access-endpoint*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetVerifiedAccessInstanceWebAcl [permission only]	Grants permission to show the Amazon 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	
GetVpnConnectionDeviceSampleConfiguration	Grants permission to download an Amazon-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*		
				ec2:Region	

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeThroughput ec2:VolumeType	
				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: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/${TagKey} ec2:RootDeviceType ec2:Tenancy	
			capacity-reservation	aws:ResourceTag/${TagKey}	
				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: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
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: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
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: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/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
ModifyInstanceEventWindow	Grants permission to modify the specified event window	Write	instance-event-window*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyInstanceMaintenanceOptions	Grants permission to modify the recovery behaviour for an instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone 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/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
ModifyInstanceMetadataDefaults	Grants permission to modify the default instance metadata service (IMDS) settings for your account in the specified Region	Write		ec2:Attribute/${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: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
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: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
ModifyInstancePlacement	Grants permission to modify the placement attributes for an instance	Write	instance*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone 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/${TagKey} ec2:RootDeviceType ec2:Tenancy	
			dedicated-host	aws:ResourceTag/${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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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}	
				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/${TagKey}	
				ec2:Region	
ModifyIpamResourceDiscovery	Grants permission to modify a resource discovery	Write	ipam-resource-discovery*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
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/${TagKey} ec2:ResourceTag/${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	
ModifyManagedPrefixList	Grants permission to modify a managed prefix list	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
				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: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:PlacementGroup ec2:ProductCode	

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	
				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: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: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
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}	
			subnet	aws:ResourceTag/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
ModifySubnetAttribute	Grants permission to modify an attribute of a subnet	Write	subnet*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone 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
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/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${TagKey} ec2:SubnetID ec2:Vpc	
				ec2:Region	
ModifyVerifiedAccessEndpoint	Grants permission to modify the configuration of a Verified Access endpoint	Write	verified-access-endpoint*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyVerifiedAccessEndpointPolicy	Grants permission to modify the specified Verified Access endpoint policy	Write	verified-access-endpoint*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ModifyVerifiedAccessGroup	Grants permission to modify the specified Verified Access Group configuration	Write	verified-access-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
			verified-access-instance	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:Region	
ModifyVerifiedAccessGroupPolicy	Grants permission to modify the specified Verified Access group policy	Write	verified-access-group*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ModifyVerifiedAccessInstance	Grants permission to modify the configuration of the specified 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
ModifyVerifiedAccessInstanceLoggingConfiguration	Grants permission to modify the logging configuration for the specified Verified Access instance	Write	verified-access-instance*	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}	
				ec2:Region	
ModifyVerifiedAccessTrustProvider	Grants permission to modify the configuration of the specified Verified Access 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
ModifyVolume	Grants permission to modify the parameters of an EBS volume	Write	volume*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:AvailabilityZone ec2:Encrypted ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:ResourceTag/${TagKey}	

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeID 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/${TagKey} ec2:ResourceTag/${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
ModifyVpcEndpoint	Grants permission to modify an attribute of a VPC endpoint	Write	vpc-endpoint*	aws:ResourceTag/${TagKey} ec2:Attribute ec2:Attribute/${AttributeName} ec2:ResourceTag/${TagKey}	
			route-table	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2:RouteTableID	

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

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

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

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

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 Amazon 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	Write	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: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:PlacementGroup ec2:ProductCode	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType	iam:PassRole

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:NewInstanceProfile ec2:PlacementGroup	

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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:InstanceBandwidthWeighting ec2:InstanceID	
				ec2:Region	
RequestSpotFleet	Grants permission to create a Spot Fleet request	Write	spot-fleet-request*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

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}	
			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/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${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/${TagKey} ec2:AvailabilityZone ec2:ResourceTag/${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 Amazon-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: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:ProductCode 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
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
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: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:IsLaunchTemplateResource ec2:LaunchTemplate ec2:ManagedResourceOperator ec2:MetadataHttpEndpoint ec2:MetadataHttpPutResponseHopLimit	

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:VolumeIops ec2:VolumeSize ec2:VolumeThroughput ec2:VolumeType	
				ec2:Region	
	SCENARIO: EC2-Classic-EBS		image* instance* security-group* volume* key-pair placement-group snapshot		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	SCENARIO: EC2-Classic-InstanceStore		image* instance* security-group* key-pair placement-group snapshot		
	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: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	

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: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	
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: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	
			license-configuration		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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/${TagKey} aws:TagKeys	
				ec2:Region	
StartNetworkInsightsAnalysis	Grants permission to start analyzing a specified path	Write	network-insights-analysis*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateTags

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:ResourceTag/${TagKey} ec2:RootDeviceType ec2:Tenancy	
				ec2:Region	
UpdateSecurityGroupRuleDescriptionsEgress	Grants permission to update descriptions for one or more outbound rules in a VPC security group	Write	security-group*	aws:ResourceTag/${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 Amazon 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-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

Resource types	ARN	Condition keys
		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:CreateDate ec2:DestinationCapacityReservationId ec2:EbsOptimized ec2:EndDate ec2:EndDateType ec2:EphemeralStorage ec2:InstanceCount

Resource types	ARN	Condition keys
		ec2:InstanceMatchCriteria ec2:InstancePlatform ec2:InstanceType ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:OutpostArn ec2:PlacementGroup ec2:Region ec2:ResourceTag/${TagKey} ec2:SourceCapacityReservationId 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
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: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:CpuOptionsAmdSevSnp ec2:EbsOptimized ec2:InstanceAutoRecovery ec2:InstanceBandwidthWeighting ec2:InstanceID ec2:InstanceMarketType ec2:InstanceMetadataTags ec2:InstanceProfile ec2:InstanceType

Resource types	ARN	Condition keys
		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/${TagKey}
ipam-pool	`arn:${Partition}:ec2::${Account}:ipam-pool/${IpamPoolId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Attribute ec2:Attribute/${AttributeName} ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
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}
ipam-resource-discovery	`arn:${Partition}:ec2::${Account}:ipam-resource-discovery/${IpamResourceDiscoveryId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
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/${TagKey}
coip-pool	`arn:${Partition}:ec2:${Region}:${Account}:coip-pool/${Ipv4PoolCoipId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
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: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}
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}

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/${TagKey}
network-acl	`arn:${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/${AttributeName} ec2:Region ec2:ResourceTag/${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:Attribute ec2:Attribute/${AttributeName} ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Region ec2:ResourceTag/${TagKey} ec2:SecurityGroupID ec2:Vpc

Resource types	ARN	Condition keys
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:Region ec2:Remove/group

Resource types	ARN	Condition keys
		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/${AttributeName} ec2:AvailabilityZone ec2:IsLaunchTemplateResource ec2:LaunchTemplate ec2:Region ec2:ResourceTag/${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-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

Resource types	ARN	Condition keys
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/${TagKey} ec2:transitGatewayPolicyTableId
transit-gateway-route-table-announcement	`arn:${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

Resource types	ARN	Condition keys
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
verified-access-endpoint	`arn:${Partition}:ec2:${Region}:${Account}:verified-access-endpoint/${VerifiedAccessEndpointId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
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/${TagKey}
verified-access-group	`arn:${Partition}:ec2:${Region}:${Account}:verified-access-group/${VerifiedAccessGroupId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${TagKey}
verified-access-instance	`arn:${Partition}:ec2:${Region}:${Account}:verified-access-instance/${VerifiedAccessInstanceId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys ec2: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/${TagKey} aws:TagKeys ec2:Region ec2:ResourceTag/${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/${AttributeName} ec2:AvailabilityZone ec2:Encrypted ec2:IsLaunchTemplateResource ec2:KmsKeyId ec2:LaunchTemplate ec2:ManagedResourceOperator ec2:ParentSnapshot ec2:Region ec2:ResourceTag/${TagKey} ec2:VolumeID ec2:VolumeIops ec2:VolumeSize

Resource types	ARN	Condition keys
		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: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:VpceServiceName ec2:VpceServiceOwner

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:VpceServicePrivateDnsName ec2:vpceMultiRegion 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-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 Amazon 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 Amazon 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 Amazon Web Services Region	String
ec2:AvailabilityZoneId	Filters access by the ID of an Availability Zone in an Amazon Web Services 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: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
ec2:DhcpOptionsID	Filters access by the ID of a dynamic host configuration protocol (DHCP) options set	String

Condition keys	Description	Type
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 Amazon FIS action	String
ec2:FisTargetArns	Filters access by the ARN of an Amazon FIS target	ArrayOfARN
ec2:GatewayType	Filters access by the gateway type for a VPN endpoint on the Amazon 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
ec2:ImageID	Filters access by the ID of an image	String

Condition keys	Description	Type
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: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: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
ec2:KmsKeyId	Filters access by the ID of an Amazon 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

Condition keys	Description	Type
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 Amazon Web Services account ID)	String
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

Condition keys	Description	Type
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
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

Condition keys	Description	Type
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 Amazon Web Services 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
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

Condition keys	Description	Type
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
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

Condition keys	Description	Type
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: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: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

Condition keys	Description	Type
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: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 Amazon Web Services account ID)	String
ec2:VpceServicePrivateDnsName	Filters access by the private DNS name 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:transitGatewayMulticastDomainId	Filters access by the ID of a transit gateway multicast domain	String

Condition keys	Description	Type
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
ec2:vpceMultiRegion	Filters access by multi region 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

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 Amazon. 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.

> **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:CapacityReservationIds autoscaling:CapacityReservationResourceGroupArns autoscaling:InstanceTypes autoscaling:LaunchConfigurationName autoscaling:LaunchTemplateVersionSpecified autoscaling:LoadBalancerNames	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				autoscaling:MaxSize autoscaling:MinSize autoscaling:TargetGroupARNs autoscaling:TrafficSourceIdentifiers autoscaling:VPCZoneIdentifiers aws:RequestTag/${TagKey} aws:TagKeys	
CreateLaunchConfiguration	Grants permission to create a launch configuration	Write	launchConfiguration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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/${TagKey} aws:TagKeys	
DeleteAutoScalingGroup	Grants permission to delete the specified Auto Scaling group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
DeleteLaunchConfiguration	Grants permission to delete the specified launch configuration	Write	launchConfiguration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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}	
DeletePolicy	Grants permission to delete the specified Auto Scaling policy	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 Amazon Web Services account	List			
DescribeAdjustmentTypes	Grants permission to describe the policy adjustment types for use with PutScalingPolicy	List			
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			

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
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}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				autoscaling:TargetGroupARNs	
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}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				autoscaling:TrafficSourceIdentifiers	
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}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnterStandby	Grants permission to move the specified instances into Standby mode	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
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}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetPredictiveScalingForecast	Grants permission to retrieve the forecast data for a predictive scaling policy	List			
PutLifecycleHook	Grants permission to create or update a lifecycle hook for the specified Auto Scaling Group	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
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}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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}	
				autoscaling:MaxSize autoscaling:MinSize	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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}	
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}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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}	
SetInstanceHealth	Grants permission to set the health status of the specified instance	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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}	
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}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TerminateInstanceInAutoScalingGroup	Grants permission to terminate the specified instance and optionally adjust the desired group size	Write	autoScalingGroup*	autoscaling:ResourceTag/${TagKey} aws:ResourceTag/${TagKey}	
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:CapacityReservationIds autoscaling:CapacityReservationResourceGroupArns autoscaling:InstanceTypes autoscaling:LaunchConfigurationName autoscaling:LaunchTemplateVersionSpecified autoscaling:MaxSize	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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:${Id}:launchConfigurationName/${LaunchConfigurationName}`	

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 Amazon 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: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
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

Condition keys	Description	Type
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
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

Condition keys	Description	Type
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 Amazon. 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.

> **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*	aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateContainerRecipe	Grants permission to create a new Container Recipe	Write	containerRecipe*	aws:RequestTag/${TagKey} aws:TagKeys	ecr:DescribeImages ecr:DescribeRepositories iam:CreateServiceLinkedRole imagebuilder:GetComponent imagebuilder:GetImage imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ssm:GetParameter
CreateDistributionConfiguration	Grants permission to create a new distribution configuration	Write	distributionConfiguration*	aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole imagebuilder:TagResource ssm:GetParameter

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateImage	Grants permission to create a new image	Write	image*	aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetContainerRecipe imagebuilder:GetDistributionConfiguration imagebuilder:GetImageRecipe imagebuilder:GetInfrastructureConfiguration imagebuilder:GetWorkflow

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					imagebuilder:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateImagePipeline	Grants permission to create a new image pipeline	Write	imagePipeline*	aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetContainerRecipe imagebuilder:GetDistributionConfiguration imagebuilder:GetImageRecipe imagebuilder:GetInfrastructureConfiguration imagebuilder:GetWorkflow

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					imagebuilder:TagResource
CreateImageRecipe	Grants permission to create a new Image Recipe	Write	imageRecipe*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeImages iam:CreateServiceLinkedRole imagebuilder:GetComponent imagebuilder:GetImage imagebuilder:TagResource ssm:GetParameter

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateInfrastructureConfiguration	Grants permission to create a new infrastructure configuration	Write	infrastructureConfiguration*	aws:RequestTag/${TagKey} aws:TagKeys imagebuilder:CreatedResourceTagKeys imagebuilder:CreatedResourceTag/<key> imagebuilder:Ec2MetadataHttpTokens imagebuilder:StatusTopicArn	iam:CreateServiceLinkedRole iam:PassRole imagebuilder:TagResource sns:Publish

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateLifecyclePolicy	Grants permission to create a new lifecycle policy	Write	lifecyclePolicy*	aws:RequestTag/${TagKey} aws:TagKeys imagebuilder:LifecyclePolicyResourceType	iam:PassRole imagebuilder:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateWorkflow	Grants permission to create a new workflow	Write	workflow*	aws:RequestTag/${TagKey} aws:TagKeys	imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext s3:GetObject s3:ListBucket
DeleteComponent	Grants permission to delete a component	Write	component*		
DeleteContainerRecipe	Grants permission to delete a container recipe	Write	containerRecipe*		
DeleteDistributionConfiguration	Grants permission to delete a distribution configuration	Write	distributionConfiguration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
GetComponent	Grants permission to view details about a component	Read	component*		kms:Decrypt
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDistributionConfiguration	Grants permission to view details about a distribution configuration	Read	distributionConfiguration*		
GetImage	Grants permission to view details about an image	Read	image*	aws:ResourceTag/${TagKey}	
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*		
GetInfrastructureConfiguration	Grants permission to view details about an infrastructure configuration	Read	infrastructureConfiguration*		
GetLifecycleExecution	Grants permission to view details about a lifecycle execution	Read	lifecycleExecution*		

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportComponent	Grants permission to import a new component	Write	component*	aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole imagebuilder:TagResource kms:Encrypt kms:GenerateDataKey kms:GenerateDataKeyWithoutPlaintext

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportDiskImage	Grants permission to import a disk image	Write	imageVersion*	aws:RequestTag/${TagKey} aws:TagKeys	iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetInfrastructureConfiguration imagebuilder:GetWorkflow imagebuilder:TagResource s3:GetObject s3:ListBucket

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportVmImage	Grants permission to import an image	Write	imageVersion*	aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeImages ec2:DescribeImportImageTasks iam:CreateServiceLinkedRole
ListComponentBuildVersions	Grants permission to list the component build versions in your account	List	componentVersion*		
ListComponents	Grants permission to list the component versions owned by or shared with your account	List			
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	imageVersion*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListImagePackages	Grants permission to return a list of packages installed on the specified image	List	image*	aws:ResourceTag/${TagKey}	
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		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	aws:ResourceTag/${TagKey}	
			containerRecipe	aws:ResourceTag/${TagKey}	
			distributionConfiguration	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			image	aws:ResourceTag/${TagKey}	
			imagePipeline	aws:ResourceTag/${TagKey}	
			imageRecipe	aws:ResourceTag/${TagKey}	
			infrastructureConfiguration	aws:ResourceTag/${TagKey}	
			lifecyclePolicy	aws:ResourceTag/${TagKey}	
			workflow	aws:ResourceTag/${TagKey}	
ListWaitingWorkflowSteps	Grants permission to list waiting workflow steps for the caller account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListWorkflowBuildVersions	Grants permission to list the workflow build versions in your account	List	workflowVersion*		
ListWorkflowExecutions	Grants permission to list workflow executions for the specified image	List	image*		
ListWorkflowStepExecutions	Grants permission to list workflow step executions for the specified workflow	List	workflowExecution*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutImageRecipePolicy	Grants permission to set the resource policy associated with an image recipe	Permissions management	imageRecipe*		
SendWorkflowStepAction	Grants permission to send an action to a workflow step	Write	image*		
			workflowStepExecution*		
StartImagePipelineExecution	Grants permission to create a new image from a pipeline	Write	imagePipeline*		iam:CreateServiceLinkedRole imagebuilder:GetImagePipeline
StartResourceStateUpdate	Grants permission to start a state update for the specified resource	Write	image*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to tag an Image Builder resource	Tagging	component	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
			containerRecipe	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			workflow	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to untag an Image Builder resource	Tagging	component	aws:ResourceTag/${TagKey} aws:TagKeys	
			containerRecipe	aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			distributionConfiguration	aws:ResourceTag/${TagKey} aws:TagKeys	
			image	aws:ResourceTag/${TagKey} aws:TagKeys	
			imagePipeline	aws:ResourceTag/${TagKey} aws:TagKeys	
			imageRecipe	aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			infrastructureConfiguration	aws:ResourceTag/${TagKey} aws:TagKeys	
			lifecyclePolicy	aws:ResourceTag/${TagKey} aws:TagKeys	
			workflow	aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateDistributionConfiguration	Grants permission to update an existing distribution configuration	Write	distributionConfiguration*		ssm:GetParameter

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateImagePipeline	Grants permission to update an existing image pipeline	Write	imagePipeline*		iam:CreateServiceLinkedRole iam:PassRole imagebuilder:GetContainerRecipe imagebuilder:GetDistributionConfiguration imagebuilder:GetImageRecipe imagebuilder:GetInfrastructureConfiguration imagebuilder:GetWorkflow

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateInfrastructureConfiguration	Grants permission to update an existing infrastructure configuration	Write	infrastructureConfiguration*	aws:ResourceTag/${TagKey} imagebuilder:CreatedResourceTagKeys imagebuilder:CreatedResourceTag/<key> imagebuilder:Ec2MetadataHttpTokens imagebuilder:StatusTopicArn	iam:PassRole sns:Publish
UpdateLifecyclePolicy	Grants permission to update an existing lifecycle policy	Write	lifecyclePolicy*	imagebuilder:LifecyclePolicyResourceType	iam:PassRole

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/${TagKey}
componentVersion	`arn:${Partition}:imagebuilder:${Region}:${Account}:component/${ComponentName}/${ComponentVersion}`	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}

Resource types	ARN	Condition keys
container Recipe	arn:${Partition}:imagebuilder:${Region}:${Account}:container-recipe/${ContainerRecipeName}/${ContainerRecipeVersion}	aws:ResourceTag/${TagKey}
imagePipeline	arn:${Partition}:imagebuilder:${Region}:${Account}:image-pipeline/${ImagePipelineName}	aws:ResourceTag/${TagKey}
infrastructureConfiguration	arn:${Partition}:imagebuilder:${Region}:${Account}:infrastructure-configuration/${ResourceId}	aws:ResourceTag/${TagKey}
kmsKey	arn:${Partition}:kms:${Region}:${Account}:key/${KeyId}	
lifecycle Execution	arn:${Partition}:imagebuilder:${Region}:${Account}:lifecycle-execution/${LifecycleExecutionId}	
lifecycle Policy	arn:${Partition}:imagebuilder:${Region}:${Account}:lifecycle-policy/${LifecyclePolicyName}	aws:ResourceTag/${TagKey}
workflow	arn:${Partition}:imagebuilder:${Region}:${Account}:workflow/${WorkflowType}/${WorkflowName}/${WorkflowVersion}/${WorkflowBuildVersion}	aws:ResourceTag/${TagKey}
workflowVersion	arn:${Partition}:imagebuilder:${Region}:${Account}:workflow/${WorkflowType}/${WorkflowName}/${WorkflowVersion}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
workflowExecution	`arn:${Partition}:imagebuilder:${Region}:${Account}:workflow-execution/${WorkflowExecutionId}`	
workflowStepExecution	`arn:${Partition}:imagebuilder:${Region}:${Account}:workflow-step-execution/${WorkflowStepExecutionId}`	

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 Amazon 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/<key>	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 EC2 Instance Connect

Amazon EC2 Instance Connect (service prefix: `ec2-instance-connect`) 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 Instance Connect
- Resource types defined by Amazon EC2 Instance Connect

- Condition keys for Amazon EC2 Instance Connect

Actions defined by Amazon EC2 Instance Connect

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 Amazon. 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.

> **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
OpenTunnel	Grants permission to establish SSH connection to an EC2 instance using EC2 Instance Connect Endpoint	Write	instance-connect-endpoint*		
			instance-connect-endpoint	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey} ec2-instance-connect:remotePort ec2-instance-connect:privateIpAddress ec2-instance-conne	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ct:MaxTunnelDuration	
SendSSHPublicKey	Grants permission to push an SSH public key to the specified EC2 instance to be used for standard SSH	Write	instance*		
				ec2:osuser	
SendSerialConsoleSSHPublicKey	Grants permission to push an SSH public key to the specified EC2 instance to be used for serial console SSH	Write	instance*		

Resource types defined by Amazon EC2 Instance Connect

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
instance	`arn:${Partition}:ec2:${Region}:${Account}:instance/${InstanceId}`	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
instance-connect-endpoint	`arn:${Partition}:ec2:${Region}:${Account}:instance-connect-endpoint/${InstanceConnectEndpointId}`	aws:ResourceTag/${TagKey} ec2:ResourceTag/${TagKey}

Condition keys for Amazon EC2 Instance Connect

Amazon EC2 Instance Connect 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 Amazon global condition context keys.

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by tags associated with the resource	String
ec2-instance-connect:maxTunnelDuration	Filters access by maximum session duration associated with the instance	Numeric
ec2-instance-connect:privateIpAddress	Filters access by private IP Address associated with the instance	IPAddress
ec2-instance-connect:remotePort	Filters access by port number associated with the instance	Numeric

Condition keys	Description	Type
ec2:ResourceTag/${TagKey}	Filters access by tags associated with the resource	String
ec2:osuser	Filters access by specifying the default user name for the AMI that you used to launch your instance	String

Actions, resources, and condition keys for Amazon EKS Auth

Amazon EKS Auth (service prefix: `eks-auth`) 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 EKS Auth
- Resource types defined by Amazon EKS Auth
- Condition keys for Amazon EKS Auth

Actions defined by Amazon EKS Auth

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 Amazon. 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.

> **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
AssumeRoleForPodIdentity	Grants permission to exchange a Kubernetes service account token for temporary Amazon credentials	Read	cluster*		

Resource types defined by Amazon EKS Auth

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}

Condition keys for Amazon EKS Auth

Amazon EKS Auth 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 Amazon global condition context keys.

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by a tag key and value pair	String

Actions, resources, and condition keys for Amazon Elastic Beanstalk

Amazon Elastic Beanstalk (service prefix: `elasticbeanstalk`) 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 Beanstalk
- Resource types defined by Amazon Elastic Beanstalk
- Condition keys for Amazon Elastic Beanstalk

Actions defined by Amazon Elastic Beanstalk

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 Amazon. 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.

> **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
AbortEnvironmentUpdate	Grants permission to cancel in-progress environment configuration update or application version deployment	Write	environment*	elasticbeanstalk:InApplication	
AddTags	Grants permission to add tags to an Elastic Beanstalk resource and to update tag values	Tagging	application		
			applicationversion		
			configurationtemplate		
			environment		
			platform		
				aws:RequestTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} aws:TagKeys	
ApplyEnvironmentManagedAction	Grants permission to apply a scheduled managed action immediately	Write	environment*	elasticbeanstalk:InApplication	
AssociateEnvironmentOperationsRole	Grants permission to associate an operations role with an environment	Write	environment*		
CheckDNSAvailability	Grants permission to check CNAME availability	Read			
ComposeEnvironments	Grants permission to create or update a group of environments, each running a separate component of a single application	Write	application*		
			applicationversion*	elasticbeanstalk:InApplication	
CreateApplication	Grants permission to create a new application	Write	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateApplicationVersion	Grants permission to create an application version for an application	Write	application*		
			applicationversion*	elasticbeanstalk:InApplication aws:RequestTag/${TagKey} aws:TagKeys	
CreateConfigurationTemplate	Grants permission to create a configuration template	Write	configurationtemplate*	elasticbeanstalk:InApplication	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				elasticbeanstalk:FromApplication elasticbeanstalk:FromApplicationVersion elasticbeanstalk:FromConfigurationTemplate elasticbeanstalk:FromEnvironment elasticbeanstalk:FromSolutionStack elasticbeanstalk:FromPlatform	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEnvironment	Grants permission to launch an environment for an application	Write	environment*	elasticbeanstalk:InApplication	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				elasticbeanstalk:FromApplicationVersion elasticbeanstalk:FromConfigurationTemplate elasticbeanstalk:FromSolutionStack elasticbeanstalk:FromPlatform aws:RequestTag/${TagKey} aws:TagKeys	
CreatePlatformVersion	Grants permission to create a new version of a custom platform	Write	platform*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStorageLocation	Grants permission to create the Amazon S3 storage location for the account	Write			
DeleteApplication	Grants permission to delete an application along with all associated versions and configurations	Write	application*		
DeleteApplicationVersion	Grants permission to delete an application version from an application	Write	applicationversion*	elasticbeanstalk:InApplication	
DeleteConfigurationTemplate	Grants permission to delete a configuration template	Write	configurationtemplate*	elasticbeanstalk:InApplication	
DeleteEnvironmentConfiguration	Grants permission to delete the draft configuration associated with the running environment	Write	environment*	elasticbeanstalk:InApplication	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeletePlatformVersion	Grants permission to delete a version of a custom platform	Write	platform*		
DescribeAccountAttributes	Grants permission to retrieve a list of account attributes, including resource quotas	Read			
DescribeApplicationVersions	Grants permission to retrieve a list of application versions stored in an Amazon Elastic Beanstalk storage bucket	List	applicationversion	elasticbeanstalk:InApplication	
DescribeApplications	Grants permission to retrieve the descriptions of existing applications	List	application		
DescribeConfigurationOptions	Grants permission to retrieve descriptions of environment configuration options	Read	configurationtemplate	elasticbeanstalk:InApplication	
			environment	elasticbeanstalk:InApplication	
			solutionstack		
DescribeConfigurationSettings	Grants permission to retrieve a description of the settings for a configuration set	Read	configurationtemplate	elasticbeanstalk:InApplication	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			environment	elasticbeanstalk:InApplication	
DescribeEnvironmentHealth	Grants permission to retrieve information about the overall health of an environment	Read	environment		
DescribeEnvironmentManagedActionHistory	Grants permission to retrieve a list of an environment's completed and failed managed actions	Read	environment	elasticbeanstalk:InApplication	
DescribeEnvironmentManagedActions	Grants permission to retrieve a list of an environment's upcoming and in-progress managed actions	Read	environment	elasticbeanstalk:InApplication	
DescribeEnvironmentResources	Grants permission to retrieve a list of Amazon resources for an environment	Read	environment	elasticbeanstalk:InApplication	
DescribeEnvironments	Grants permission to retrieve descriptions for existing environments	List	environment	elasticbeanstalk:InApplication	
DescribeEvents	Grants permission to retrieve a list of event descriptions matching a set of criteria	Read	application		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			applicationversion	elasticbeanstalk:InApplication	
			configurationtemplate	elasticbeanstalk:InApplication	
			environment	elasticbeanstalk:InApplication	
DescribeInstancesHealth	Grants permission to retrieve more detailed information about the health of environment instances	Read	environment		
DescribePlatformVersion	Grants permission to retrieve a description of a managed platform version	Read	platform		
DisassociateEnvironmentOperationsRole	Grants permission to disassociate an operations role with an environment	Write	environment*		
ListAvailableSolutionStacks	Grants permission to retrieve a list of the available solution stack names	List	solutionstack		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPlatformBranches	Grants permission to retrieve a list of the available platform branches	List			
ListPlatformVersions	Grants permission to retrieve a list of the available platforms	List	platform		
ListTagsForResource	Grants permission to retrieve a list of tags of an Elastic Beanstalk resource	Read	application		
			applicationversion		
			configurationtemplate		
			environment		
			platform		
PutInstanceStatistics	Grants permission to submit instance statistics for enhanced health	Write	application*		
			environment*		
RebuildEnvironment	Grants permission to delete and recreate all of the Amazon resources for an environment and to force a restart	Write	environment*	elasticbeanstalk:InApplication	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RemoveTags	Grants permission to remove tags from an Elastic Beanstalk resource	Tagging	application		
			applicationversion		
			configurationtemplate		
			environment		
			platform		
				aws:TagKeys	
RequestEnvironmentInfo	Grants permission to initiate a request to compile information of the deployed environment	Read	environment*	elasticbeanstalk:InApplication	
RestartAppServer	Grants permission to request an environment to restart the application container server running on each Amazon EC2 instance	Write	environment*	elasticbeanstalk:InApplication	
RetrieveEnvironmentInfo	Grants permission to retrieve the compiled information from a RequestEnvironmentInfo request	Read	environment*	elasticbeanstalk:InApplication	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SwapEnvironmentCNAMEs	Grants permission to swap the CNAMEs of two environments	Write	environment*	elasticbeanstalk:InApplication	
				elasticbeanstalk:FromEnvironment	
TerminateEnvironment	Grants permission to terminate an environment	Write	environment*	elasticbeanstalk:InApplication	
UpdateApplication	Grants permission to update an application with specified properties	Write	application*		
UpdateApplicationResourceLifecycle	Grants permission to update the application version lifecycle policy associated with the application	Write	application*		
UpdateApplicationVersion	Grants permission to update an application version with specified properties	Write	applicationversion*	elasticbeanstalk:InApplication	
UpdateConfigurationTemplate	Grants permission to update a configuration template with specified properties or configuration option values	Write	configurationtemplate*	elasticbeanstalk:InApplication	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				elasticbeanstalk:FromApplication elasticbeanstalk:FromApplicationVersion elasticbeanstalk:FromConfigurationTemplate elasticbeanstalk:FromEnvironment elasticbeanstalk:FromSolutionStack elasticbeanstalk:FromPlatform	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateEnvironment	Grants permission to update an environment	Write	environment*	elasticbeanstalk:InApplication	
				elasticbeanstalk:FromApplicationVersion elasticbeanstalk:FromConfigurationTemplate elasticbeanstalk:FromSolutionStack elasticbeanstalk:FromPlatform	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateTagsForResource	Doesn't grant permission to update tags. To grant permission to add tags to an Elastic Beanstalk resource, remove tags, and to update tag values, specify elasticbeanstalk:AddTags and elasticbeanstalk:RemoveTags	Tagging	application		
			applicationversion		
			configurationtemplate		
			environment		
			platform		
				aws:RequestTag/${TagKey} aws:TagKeys	
ValidateConfigurationSettings	Grants permission to check the validity of a set of configuration settings for a configuration template or an environment	Read	configurationtemplate	elasticbeanstalk:InApplication	
			environment	elasticbeanstalk:InApplication	

Resource types defined by Amazon Elastic Beanstalk

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:${Partition}:elasticbeanstalk:${Region}:${Account}:application/${ApplicationName}`	aws:ResourceTag/${TagKey}
applicationversion	`arn:${Partition}:elasticbeanstalk:${Region}:${Account}:applicationversion/${ApplicationName}/${VersionLabel}`	aws:ResourceTag/${TagKey} elasticbeanstalk:InApplication
configurationtemplate	`arn:${Partition}:elasticbeanstalk:${Region}:${Account}:configurationtemplate/${ApplicationName}/${TemplateName}`	aws:ResourceTag/${TagKey} elasticbeanstalk:InApplication
environment	`arn:${Partition}:elasticbeanstalk:${Region}:${Account}:environment/${ApplicationName}/${EnvironmentName}`	aws:ResourceTag/${TagKey} elasticbeanstalk:InApplication
solutionstack	`arn:${Partition}:elasticbeanstalk:${Region}::solutionstack/${SolutionStackName}`	

Resource types	ARN	Condition keys
platform	`arn:${Partition}:elasticbeanstalk:${Region}::platform/${PlatformNameWithVersion}`	

Condition keys for Amazon Elastic Beanstalk

Amazon Elastic Beanstalk 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 Amazon global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters actions based on the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters actions based on tag key-value pairs attached to the resource	String
aws:TagKeys	Filters actions based on the presence of tag keys in the request	ArrayOfString
elasticbeanstalk:FromApplication	Filters access by an application as a dependency or a constraint on an input parameter	ARN
elasticbeanstalk:FromApplicationVersion	Filters access by an application version as a dependency or a constraint on an input parameter	ARN

Condition keys	Description	Type
elasticbeanstalk:FromConfigurationTemplate	Filters access by a configuration template as a dependency or a constraint on an input parameter	ARN
elasticbeanstalk:FromEnvironment	Filters access by an environment as a dependency or a constraint on an input parameter	ARN
elasticbeanstalk:FromPlatform	Filters access by a platform as a dependency or a constraint on an input parameter	ARN
elasticbeanstalk:FromSolutionStack	Filters access by a solution stack as a dependency or a constraint on an input parameter	ARN
elasticbeanstalk:InApplication	Filters access by the application that contains the resource that the action operates on	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 Amazon. 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.

> **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}	
PutSnapshotBlock	Grants permission to write a block of data to a snapshot created by the StartSnapshot operation	Write	snapshot*		
				aws:ResourceTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey}	
StartSnapshot	Grants permission to create a new EBS snapshot	Write	snapshot		
				aws:RequestTag/${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 Amazon 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

Condition keys	Description	Type
ebs:Description	Filters access by the description of the snapshot being created	String
ebs:ParentSnapshot	Filters access by the ID of the parent snapshot	String
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 Amazon. 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.

> **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	Read	repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	image layers in a specified registry and 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 [permission only]	Grants permission to retrieve the image from the upstream registry and import it to your private registry	Write	repository*		
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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRepository	Grants permission to create an image repository	Write	repository*		ecr:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	
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*		

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

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*		
InitiateLayerUpload	Grants permission to notify Amazon ECR that you intend to upload an image layer	Write	repository*		
ListImages	Grants permission to list all the image IDs for a given repository	List	repository*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
PutLifecyclePolicy	Grants permission to create or update a lifecycle policy	Write	repository*		
PutRegistryPolicy	Grants permission to update the registry policy	Permissions management			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutRegistryScanningConfiguration	Grants permission to update registry scanning configuration	Write			
PutReplicationConfiguration	Grants permission to update the replication configuration for the registry	Write			iam:CreateServiceLinkedRole
ReplicateImage [permission only]	Grants permission to replicate images to the destination registry	Write	repository*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag an Amazon ECR resource	Tagging	repository*		
				aws:TagKeys	
UpdatePullThroughCacheRule	Grants permission to update the pull-through cache rule	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 Amazon 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
ecr:AccountSetting	Filters access by the ECR account setting name	String

Condition keys	Description	Type
ecr:ResourceTag/${TagKey}	Filters access by tag-value associated with the resource	String

Actions, resources, and condition keys for Amazon Elastic Container Service

Amazon Elastic Container Service (service prefix: `ecs`) 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 Service
- Resource types defined by Amazon Elastic Container Service
- Condition keys for Amazon Elastic Container Service

Actions defined by Amazon Elastic Container 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 Amazon. 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.

> **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
CreateCapacityProvider	Grants permission to create a new capacity provider. Capacity providers are associated with an Amazon ECS cluster and are used in capacity provider strategies to facilitate cluster auto scaling	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCluster	Grants permission to create a new Amazon ECS cluster	Write	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys ecs:capacity-provider ecs:fargate-ephemeral-storage-kms-key	
CreateService	Grants permission to run and maintain a desired number of tasks from a specified task definition via service creation	Write	service*	ecs:cluster aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys ecs:capacity-provider ecs:task-definition ecs:enable-ebs-volumes ecs:enable-execute-command ecs:enable-service-connect ecs:namespace	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ecs:enable-vpc-lattice ecs:enable-ecs-managed-tags ecs:propagate-tags ecs:auto-assign-public-ip ecs:subnet ecs:task-cpu ecs:task-memory	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTaskSet	Grants permission to create a new Amazon ECS task set	Write		aws:RequestTag/${TagKey} aws:TagKeys ecs:cluster ecs:capacity-provider ecs:service ecs:task-definition	
DeleteAccountSetting	Grants permission to modify the ARN and resource ID format of a resource for a specified IAM user, IAM role, or the root user for an account. You can specify whether the new ARN and resource ID format are disabled for new resources that are created	Write		ecs:account-setting	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAttributes	Grants permission to delete one or more custom attributes from an Amazon ECS resource	Write	container-instance*		
				aws:ResourceTag/${TagKey} ecs:cluster	
DeleteCapacityProvider	Grants permission to delete the specified capacity provider	Write	capacity-provider*		
				aws:ResourceTag/${TagKey}	
DeleteCluster	Grants permission to delete the specified cluster	Write	cluster*		
				aws:ResourceTag/${TagKey}	
DeleteService	Grants permission to delete a specified service within a cluster	Write	service*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} ecs:cluster	
DeleteTaskDefinitions	Grants permission to delete the specified task definitions by family and revision	Write	task-definition*		
				aws:ResourceTag/${TagKey}	
DeleteTaskSet	Grants permission to delete the specified task set	Write	task-set*		
				aws:ResourceTag/${TagKey} ecs:cluster ecs:service	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeregisterContainerInstance	Grants permission to deregister an Amazon ECS container instance from the specified cluster	Write	cluster*		
				aws:ResourceTag/${TagKey}	
DeregisterTaskDefinition	Grants permission to deregister the specified task definition by family and revision	Write			
DescribeCapacityProviders	Grants permission to describe one or more Amazon ECS capacity providers	Read	capacity-provider*		
				aws:ResourceTag/${TagKey}	
DescribeClusters	Grants permission to describes one or more of your clusters	Read	cluster*		
				aws:ResourceTag/${TagKey}	
DescribeContainerInstances	Grants permission to describes Amazon ECS container instances	Read	container-instance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} ecs:cluster	
DescribeServiceDeployments	Grants permission to describe one or more of your service deployments	Read	service*	ecs:cluster aws:ResourceTag/${TagKey}	
			service-deployment*	ecs:cluster ecs:service aws:ResourceTag/${TagKey}	
DescribeServiceRevisions	Grants permission to describe one or more of your service revisions	Read	service*	ecs:cluster aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			service-revision*	ecs:cluster ecs:service aws:ResourceTag/${TagKey}	
DescribeServices	Grants permission to describe the specified services running in your cluster	Read	service*		
				aws:ResourceTag/${TagKey} ecs:cluster	
DescribeTaskDefinition	Grants permission to describe a task definition. You can specify a family and revision to find information about a specific task definition, or you can simply specify the family to find the latest ACTIVE revision in that family	Read			
DescribeTaskSets	Grants permission to describe Amazon ECS task sets	Read	task-set*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} ecs:cluster ecs:service	
DescribeTasks	Grants permission to describe a specified task or tasks	Read	task*		
				aws:ResourceTag/${TagKey} ecs:cluster	
DiscoverPollEndpoint	Grants permission to get an endpoint for the Amazon ECS agent to poll for updates	Write			
ExecuteCommand	Grants permission to run a command remotely on an Amazon ECS container	Write	cluster*		
			task*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} ecs:cluster ecs:container-name ecs:task	
GetTaskProtection	Grants permission to retrieve the protection status of tasks in an Amazon ECS service	Read	task*		
				aws:ResourceTag/${TagKey} ecs:cluster	
ListAccountSettings	Grants permission to list the account settings for an Amazon ECS resource for a specified principal	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAttributes	Grants permission to lists the attributes for Amazon ECS resources within a specified target type and cluster	List	cluster*		
				aws:ResourceTag/${TagKey}	
ListClusters	Grants permission to get a list of existing clusters	List			
ListContainerInstances	Grants permission to get a list of container instances in a specified cluster	List	cluster*		
				aws:ResourceTag/${TagKey}	
ListServiceDeployments	Grants permission to get a list of service deployments for a specified service	List	service*	aws:ResourceTag/${TagKey} ecs:cluster	
ListServices	Grants permission to get a list of services that are running in a specified cluster	List		ecs:cluster	
ListServicesByNamespace	Grants permission to get a list of services that are running in a specified Amazon Web Services Cloud Map Namespace	List		ecs:namespace	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to get a list of tags for the specified resource	Read	capacity-provider		
			cluster		
			container-instance		
			service		
			task		
			task-definition		
			task-set		
				aws:ResourceTag/${TagKey}	
ListTaskDefinitionFamilies	Grants permission to get a list of task definition families that are registered to your account (which may include task definition families that no longer have any ACTIVE task definitions)	List			
ListTaskDefinitions	Grants permission to get a list of task definitions that are registered to your account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTasks	Grants permission to get a list of tasks for a specified cluster	List	container-instance*		
				aws:ResourceTag/${TagKey} ecs:cluster	
Poll [permission only]	Grants permission to an agent to connect with the Amazon ECS service to report status and get commands	Write	container-instance*		
				ecs:cluster	
PutAccountSetting	Grants permission to modify the ARN and resource ID format of a resource for a specified IAM user, IAM role, or the root user for an account. You can specify whether the new ARN and resource ID format are enabled for new resources that are created. Enabling this setting is required to use new Amazon ECS features such as resource tagging	Write		ecs:account-setting	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutAccountSettingDefault	Grants permission to modify the ARN and resource ID format of a resource type for all IAM users on an account for which no individual account setting has been set. Enabling this setting is required to use new Amazon ECS features such as resource tagging	Write		ecs:account-setting	
PutAttributes	Grants permission to create or update an attribute on an Amazon ECS resource	Write	container-instance*		
				aws:ResourceTag/${TagKey} ecs:cluster	
PutClusterCapacityProviders	Grants permission to modify the available capacity providers and the default capacity provider strategy for a cluster	Write	cluster*		
				aws:ResourceTag/${TagKey} ecs:capacity-provider	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterContainerInstance	Grants permission to register an EC2 instance into the specified cluster	Write	cluster*		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
RegisterTaskDefinition	Grants permission to register a new task definition from the supplied family and container Definitions	Write	task-definition*	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys ecs:compute-compatibility ecs:privileged ecs:task-cpu ecs:task-memory	
RunTask	Grants permission to start a task using random placement and the default Amazon ECS scheduler	Write	task-definition*		iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys ecs:cluster ecs:capacity-provider ecs:enable-ebs-volumes ecs:enable-execute-command	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartTask	Grants permission to start a new task from the specified task definition on the specified container instance or instances	Write	task-definition*		iam:PassRole
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys ecs:cluster ecs:container-instances ecs:enable-ebs-volumes ecs:enable-execute-command	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartTelemetrySession	Grants permission to start a telemetry session	Write	container-instance*		
				ecs:cluster	
StopServiceDeployment	Grants permission to stop an ongoing service deployment	Write	service*	ecs:cluster aws:ResourceTag/${TagKey}	
			service-deployment*	ecs:cluster ecs:service aws:ResourceTag/${TagKey}	
StopTask	Grants permission to stop a running task	Write	task*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} ecs:cluster	
SubmitAttachmentStateChanges	Grants permission to send an acknowledgement that attachments changed states	Write	cluster*		
				aws:ResourceTag/${TagKey}	
SubmitContainerStateChange	Grants permission to send an acknowledgement that a container changed states	Write	cluster*		
				aws:ResourceTag/${TagKey}	
SubmitTaskStateChange	Grants permission to send an acknowledgement that a task changed states	Write	cluster*		
				aws:ResourceTag/${TagKey}	
TagResource	Grants permission to tag the specified resource	Tagging	capacity-provider		
			cluster		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			container-instance		
			service		
			task		
			task-definition		
			task-set		
				aws:TagKeys aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} ecs:CreateAction	
UntagResource	Grants permission to untag the specified resource	Tagging	capacity-provider		
			cluster		
			container-instance		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			service		
			task		
			task-definition		
			task-set		
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCapacityProvider	Grants permission to update the specified capacity provider	Write	capacity-provider*		
				aws:ResourceTag/${TagKey}	
UpdateCluster	Grants permission to modify the configuration or settings to use for a cluster	Write	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} ecs:fargate-ephemeral-storage-kms-key	
UpdateClusterSettings	Grants permission to modify the settings to use for a cluster	Write	cluster*		
				aws:ResourceTag/${TagKey}	
UpdateContainerAgent	Grants permission to update the Amazon ECS container agent on a specified container instance	Write	container-instance*		
				aws:ResourceTag/${TagKey} ecs:cluster	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateContainerInstancesState	Grants permission to the user to modify the status of an Amazon ECS container instance	Write	container-instance*		
				aws:ResourceTag/${TagKey} ecs:cluster	
UpdateService	Grants permission to modify the parameters of a service	Write	service*	ecs:cluster aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ecs:capacity-provider ecs:enable-ebs-volumes ecs:enable-execute-command ecs:enable-service-connect ecs:namespace ecs:task-definition ecs:enable-vpc-lattice ecs:enable-ecs-managed-tags	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ecs:propagate-tags ecs:auto-assign-public-ip ecs:subnet ecs:task-cpu ecs:task-memory	
UpdateServicePrimaryTaskSet	Grants permission to modify the primary task set used in a service	Write	service*		
				aws:ResourceTag/${TagKey} ecs:cluster	
UpdateTaskProtection	Grants permission to modify the protection status of a task	Write	task*		
				aws:ResourceTag/${TagKey} ecs:cluster	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateTaskSet	Grants permission to update the specified task set	Write	task-set*		
				aws:ResourceTag/${TagKey} ecs:cluster ecs:service	

Resource types defined by Amazon Elastic Container 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:${Partition}:ecs:${Region}:${Account}:cluster/${ClusterName}`	aws:ResourceTag/${TagKey} ecs:ResourceTag/${TagKey}
container-instance	`arn:${Partition}:ecs:${Region}:${Account}:container-instance/${ClusterName}/${ContainerInstanceId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
		ecs:ResourceTag/${TagKey}
service	arn:${Partition}:ecs:${Region}:${Account}:service/${ClusterName}/${ServiceName}	aws:ResourceTag/${TagKey} ecs:ResourceTag/${TagKey}
service-deployment	arn:${Partition}:ecs:${Region}:${Account}:service-deployment/${ClusterName}/${ServiceName}/${ServiceDeploymentId}	aws:ResourceTag/${TagKey} ecs:cluster ecs:service
service-revision	arn:${Partition}:ecs:${Region}:${Account}:service-revision/${ClusterName}/${ServiceName}/${ServiceRevisionId}	aws:ResourceTag/${TagKey} ecs:cluster ecs:service
task	arn:${Partition}:ecs:${Region}:${Account}:task/${ClusterName}/${TaskId}	aws:ResourceTag/${TagKey} ecs:ResourceTag/${TagKey}
task-definition	arn:${Partition}:ecs:${Region}:${Account}:task-definition/${TaskDefinitionFamilyName}:${TaskDefinitionRevisionNumber}	aws:ResourceTag/${TagKey} ecs:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
capacity-provider	`arn:${Partition}:ecs:${Region}:${Account}:capacity-provider/${CapacityProviderName}`	aws:ResourceTag/${TagKey} ecs:ResourceTag/${TagKey}
task-set	`arn:${Partition}:ecs:${Region}:${Account}:task-set/${ClusterName}/${ServiceName}/${TaskSetId}`	aws:ResourceTag/${TagKey} ecs:ResourceTag/${TagKey}

Condition keys for Amazon Elastic Container Service

Amazon Elastic Container 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 Amazon 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

Condition keys	Description	Type
ecs:CreateAction	Filters access by the name of a resource-creating API action	String
ecs:ResourceTag/${TagKey}	Filters access by the tag key-value pairs attached to the resource	String
ecs:account-setting	Filters access by the Amazon ECS account setting name	String
ecs:auto-assign-public-ip	Filters access by the public IP assignment configuration of your Amazon ECS task or Amazon ECS service that uses awsvpc network mode	Bool
ecs:capacity-provider	Filters access by the ARN of an Amazon ECS capacity provider	ArrayOfARN
ecs:cluster	Filters access by the ARN of an Amazon ECS cluster	ARN
ecs:compute-compatibility	Filters access by the required compatibilities field provided in the request	ArrayOfString
ecs:container-instances	Filters access by the ARN of an Amazon ECS container instance	ARN
ecs:container-name	Filters access by the name of an Amazon ECS container which is defined in the ECS task definition	String
ecs:enable-ebs-volumes	Filters access by the Amazon ECS managed Amazon EBS volume capability of your ECS task or service	String
ecs:enable-ecs-managed-tags	Filters access by the enableECSManagedTags configuration of your Amazon ECS task or Amazon ECS service	Bool
ecs:enable-execute-command	Filters access by the execute-command capability of your Amazon ECS task or Amazon ECS service	String

Condition keys	Description	Type
ecs:enable-service-connect	Filters access by the enable field value in the Service Connect configuration	String
ecs:enable-vpc-lattice	Filters access by the VPC lattice capability of your Amazon ECS service	String
ecs:fargate-ephemeral-storage-kms-key	Filters access by the Amazon KMS key id provided in the request	String
ecs:namespace	Filters access by the ARN of Amazon Web Services Cloud Map namespace which is defined in the Service Connect Configuration	ARN
ecs:privileged	Filters access by the privileged field provided in the request	String
ecs:propagate-tags	Filters access by the tag propagation configuration of your Amazon ECS task or Amazon ECS service	String
ecs:service	Filters access by the ARN of an Amazon ECS service	ARN
ecs:subnet	Filters access by the subnet configuration of your Amazon ECS task or Amazon ECS service that uses awsvpc network mode	ArrayOfString
ecs:task	Filters access by the ARN of an Amazon ECS task	ARN
ecs:task-cpu	Filters access by the task cpu, as an integer with 1024 = 1 vCPU, provided in the request	Numeric
ecs:task-definition	Filters access by the ARN of an Amazon ECS task definition	ARN
ecs:task-memory	Filters access by the task memory, as an integer representing MiB, provided in the request	Numeric

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 Amazon. 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.

> **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:AccessedV	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				iaMountTarget	
ClientRootAccess [permission only]	Grants permission to allow an NFS client root-access to a file system	Write	file-system*		
				elasticfilesystem:AccessPointArn elasticfilesystem:AccessedViaMountTarget	
ClientWrite [permission only]	Grants permission to allow an NFS client write-access to a file system	Write	file-system*		
				elasticfilesystem:AccessPointArn elasticfilesystem:AccessedViaMountTarget	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAccessPoint	Grants permission to create an access point for the specified file system	Write	file-system*		elasticfilesystem:TagResource
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateFileSystem	Grants permission to create a new, empty file system	Write		aws:RequestTag/${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*		

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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			
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 Amazon Web Services account in the Amazon region of the endpoint that is being called	List	file-system		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
			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 Amazon Web Services account in the Amazon 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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
PutBackupPolicy	Grants permission to enable or disable automatic backups with Amazon 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*		

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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 Amazon 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

Condition keys	Description	Type
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 Amazon. 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.

> **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 Amazon 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 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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				eks:issuerUrl	
CreateAccessEntry	Grants permission to create an Amazon EKS access entry	Write	cluster*		
				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	

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	
CreateEksAnywhereSubscription	Grants permission to create an EKS Anywhere subscription	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateFargateProfile	Grants permission to create an Amazon Fargate profile	Write	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNodegroup	Grants permission to create an Amazon EKS Nodegroup	Write	cluster*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePodIdentityAssociation	Grants permission to create an EKS Pod Identity association	Write	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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		
DeleteCluster	Grants permission to delete an Amazon EKS cluster	Write	cluster*		
DeleteEksAnywhereSubscription	Grants permission to describe an EKS Anywhere subscription	Write	eks-anywhere-subscription*		
DeleteFargateProfile	Grants permission to delete an Amazon 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*		

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeFargateProfile	Grants permission to retrieve descriptive information about an Amazon 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*		
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		
			nodegroup		
DisassociateAccessPolicy	Grants permission to disassociate an Amazon EKS access policy from an Amazon EKS acces entry	Write	access-entry*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				eks:policyArn eks:namespaces eks:accessScope	
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 Amazon Web Services 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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListClusters	Grants permission to list the Amazon EKS clusters in your Amazon Web Services account (in the specified or default region)	List			
ListEksAnywhereSubscriptions	Grants permission to list EKS Anywhere subscriptions	List			
ListFargateProfiles	Grants permission to list the Amazon Fargate profiles in your Amazon Web Services account (in the specified or default region) associated with a given cluster	List	cluster*		
ListIdentityProviderConfigs	Grants permission to list the Idp configs in your Amazon Web Services 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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListNodegroups	Grants permission to list the Amazon EKS nodegroups in your Amazon Web Services 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		
			cluster		
			eks-anywhere-subscription		
			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		
			nodegroup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterCluster	Grants permission to register an External cluster	Write		aws:RequestTag/${TagKey} aws:TagKeys	
TagResource	Grants permission to tag the specified resource	Tagging	access-entry		
			addon		
			cluster		
			eks-anywhere-subscription		
			fargateprofile		
			identityproviderconfig		
			nodegroup		
			podidentityassociation		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag the specified resource	Tagging	access-entry		
			addon		
			cluster		
			eks-anywhere-subscription		
			fargateprofile		
			identityproviderconfig		
			nodegroup		
			podidentityassociation		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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		
UpdateClusterConfig	Grants permission to update Amazon EKS cluster configurations (eg: API server endpoint access)	Write	cluster*		
				eks:authenticationMode eks:supportType eks:computeConfigEnabled eks:elasticLoadBalancingEnabled eks:blockStorageEnabled	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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}
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

Resource types	ARN	Condition keys
		eks:kubernetesGroups eks:principalArn eks:username
access-policy	`arn:${Partition}:eks::aws:cluster-access-policy/${AccessPolicyName}`	

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 Amazon 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: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 Amazon Elastic Load Balancing

Amazon 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 Amazon Elastic Load Balancing
- Resource types defined by Amazon Elastic Load Balancing

- Condition keys for Amazon Elastic Load Balancing

Actions defined by Amazon 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 Amazon. 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.

> **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} elasticloadbalancing:CreateAction	
ApplySecurityGroupsToLoadBalancer	Grants permission to associate one or more security groups with your load	Write	loadbalancer*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	balancer in a virtual private cloud (VPC)			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 Amazon 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 Amazon Elastic Load Balancing

Amazon 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 Amazon 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 Amazon Elastic Load Balancing V2

Amazon 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 Amazon Elastic Load Balancing V2
- Resource types defined by Amazon Elastic Load Balancing V2
- Condition keys for Amazon Elastic Load Balancing V2

Actions defined by Amazon 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 Amazon. 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.

> **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/${TagKey} elasticloadbalancing:ResourceTag/${TagKey}	

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	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}	
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 Amazon Web Services 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	Read			
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 Amazon 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 Amazon Elastic Load Balancing V2

Amazon 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 Amazon 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 Amazon. 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.

> **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
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		
			studio		
				aws:RequestTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} aws:TagKeys elasticmapreduce:RequestTag/${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 Amazon Web Services 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 Amazon Web Services 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 Amazon Identity and Access Management (IAM) users in the Amazon Web Services 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 Amazon 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 Amazon 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 ElastiCache

Amazon ElastiCache (service prefix: `elasticache`) 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 ElastiCache
- Resource types defined by Amazon ElastiCache
- Condition keys for Amazon ElastiCache

Actions defined by Amazon ElastiCache

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 Amazon. 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.

> **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**
>
> When you create an ElastiCache policy in IAM you must use the "*" wildcard character for the Resource block. For information about using the following ElastiCache API actions in an IAM policy, see ElastiCache Actions and IAM in the *Amazon ElastiCache User Guide*.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddTagsToResource	Grants permission to add tags to an ElastiCache resource	Tagging	cluster		
			parametergroup		
			replicationgroup		
			reserved-instance		
			securitygroup		
			serverlesscache		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			serverlessscachesnapshot		
			snapshot		
			subnetgroup		
			user		
			usergroup		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
AuthorizeCacheSecurityGroupIngress	Grants permission to authorize an EC2 security group on a ElastiCache security group	Write	securitygroup*		ec2:AuthorizeSecurityGroupIngress

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
BatchApplyUpdateAction	Grants permission to apply ElastiCache service updates to sets of clusters and replication groups	Write	cluster		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs s3:GetObject
			replicationgroup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
BatchStopUpdateAction	Grants permission to stop ElastiCache service updates from being executed on a set of clusters	Write	cluster		
			replicationgroup		
				aws:ResourceTag/${TagKey}	
CompleteMigration	Grants permission to complete an online migration of data from hosted Redis on Amazon EC2 to ElastiCache	Write	cluster		
			replicationgroup		
				aws:ResourceTag/${TagKey}	
Connect	Grants permission to connect as a specified ElastiCache user to an ElastiCache Replication Group or ElastiCache serverless cache	Write	user*		
			replicationgroup		
			serverlesscache		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
CopyServerlessCacheSnapshot	Grants permission to make a copy of an existing serverless cache snapshot	Write	serverlessscachesnapshot*	aws:ResourceTag/${TagKey} elasticache:KmsKeyId	elasticache:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CopySnapshot	Grants permission to make a copy of an existing snapshot	Write	snapshot*		elasticache:AddTagsToResource s3:DeleteObject s3:GetBucketAcl s3:PutObject
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys elasticache:KmsKeyId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCacheCluster	Grants permission to create a cache cluster	Write	parameter group*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs elasticache:AddTagsToResource s3:GetObject

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			cluster	aws:RequestTag/${TagKey} aws:TagKeys elasticache:CacheNodeType elasticache:EngineVersion elasticache:EngineType elasticache:MultiAZEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				elasticache:CacheParameterGroupName	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			replicationgroup	elasticache:CacheNodeType elasticache:EngineVersion elasticache:EngineType elasticache:MultiAZEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:CacheParameterGroupName	
			securitygroup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot		
			subnetgroup		
				aws:ResourceTag/${TagKey}	
CreateCacheParameterGroup	Grants permission to create a parameter group	Write	parameter group*		elasticache:AddTagsToResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys elasticache:CacheParameterGroupName	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCacheSecurityGroup	Grants permission to create a cache security group	Write	securitygroup*		elasticache:AddTagsToResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateCacheSubnetGroup	Grants permission to create a cache subnet group	Write	subnetgroup*		elasticache:AddTagsToResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateGlobalReplicationGroup	Grants permission to create a global replication group	Write	globalreplicationgroup*		
			replicationgroup*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateReplicationGroup	Grants permission to create a replication group	Write	parameergroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs elasticache:AddTagsToResource s3:GetObject
			cluster		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			globalreplicationgroup	elasticache:NumNodeGroups elasticache:CacheNodeType elasticache:ReplicasPerNodeGroup elasticache:EngineVersion elasticache:EngineType elasticache:AtRestEncryptionEnabled elasticache:TransitEncryptionEnabled elasticache:AutomaticFailov	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				erEnabled elasticache:MultiAZEnabled elasticache:ClusterModeEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:KmsKeyId elasticache:CacheParameterGroupName	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			replicationgroup	aws:RequestTag/${TagKey} aws:TagKeys elasticache:NumNodeGroups elasticache:CacheNodeType elasticache:ReplicasPerNodeGroup elasticache:EngineVersion elasticache:EngineType elasticache:AtRestEncryptionEnabled	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				elasticache:TransitEncryptionEnabled elasticache:AutomaticFailoverEnabled elasticache:MultiAZEnabled elasticache:ClusterModeEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:KmsKeyId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				elasticache:CacheParameterGroupName	
			securitygroup		
			snapshot		
			subnetgroup		
			usergroup		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateServerlessCache	Grants permission to create a serverless cache	Write	serverlessscache*	aws:ResourceTag/${TagKey} elasticache:EngineType elasticache:EngineVersion elasticache:SnapshotRetentionLimit elasticache:KmsKeyId elasticache:MinimumDataStorage elasticache:MaximumDataStorage elasticache:DataSt	ec2:CreateTags ec2:CreateVpcEndpoint ec2:DeleteVpcEndpoints ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeTags ec2:DescribeVpcEndpoints ec2:DescribeVpcs elasticache:AddTagsToResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				orageUnit elasticache:MinimumECPUPerSecond elasticache:MaximumECPUPerSecond	s3:GetObject
			serverlessscachesnapshot	aws:ResourceTag/${TagKey}	
			snapshot	aws:ResourceTag/${TagKey}	
			usergroup	aws:ResourceTag/${TagKey}	
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateServerlessCacheSnapshot	Grants permission to create a copy of a serverless cache at a specific moment in time	Write	serverlesscache*	aws:ResourceTag/${TagKey}	elasticache:AddTagsToResource
			serverlesscachesnapshot*	aws:ResourceTag/${TagKey} elasticache:KmsKeyId	
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSnapshot	Grants permission to create a copy of an entire Redis cluster at a specific moment in time	Write	snapshot*	aws:RequestTag/${TagKey} aws:TagKeys elasticache:KmsKeyId	elasticache:AddTagsToResource s3:DeleteObject s3:GetBucketAcl s3:PutObject
			cluster		
			replicationgroup		
				aws:ResourceTag/${TagKey}	
CreateUser	Grants permission to create a user for Redis. Users are supported from Redis 6.0 onwards	Write	user*		elasticache:AddTagsToResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys elasticache:UserAuthenticationMode	
CreateUserGroup	Grants permission to create a user group for Redis. Groups are supported from Redis 6.0 onwards	Write	user*		elasticache:AddTagsToResource
			usergroup*	aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
DecreaseNodeGroupsInGlobalReplicationGroup	Grants permission to decrease the number of node groups in global replication groups	Write	globalreplicationgroup*		
				elasticache:NumNodeGroups	
DecreaseReplicaCount	Grants permission to decrease the number of replicas in a Redis (cluster mode disabled) replication group or the number of replica nodes in one or more node groups (shards) of a Redis (cluster mode enabled) replication group	Write	replicationgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} elasticache:ReplicasPerNodeGroup	
DeleteCacheCluster	Grants permission to delete a previously provisioned cluster	Write	cluster*	aws:ResourceTag/${TagKey}	ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
			snapshot		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteCacheParameterGroup	Grants permission to delete the specified cache parameter group	Write	parameergroup*		
				aws:ResourceTag/${TagKey} elasticache:CacheParameterGroupName	
DeleteCacheSecurityGroup	Grants permission to delete a cache security group	Write	securitygroup*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteCacheSubnetGroup	Grants permission to delete a cache subnet group	Write	subnetgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey}	
DeleteGlobalReplicationGroup	Grants permission to delete an existing global replication group	Write	globalreplicationgroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteReplicationGroup	Grants permission to delete an existing replication group	Write	replicationgroup*	aws:ResourceTag/${TagKey}	ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
			snapshot		
DeleteServerlessCache	Grants permission to delete a serverless cache	Write	serverlesscache*	aws:ResourceTag/${TagKey}	ec2:DescribeTags
			serverlesscachesnapshot		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteServerlessCacheSnapshot	Grants permission to delete a serverless cache snapshot	Write	serverlessscachesnapshot*	aws:ResourceTag/${TagKey}	
DeleteSnapshot	Grants permission to delete an existing snapshot	Write	snapshot*		
				aws:ResourceTag/${TagKey}	
DeleteUser	Grants permission to delete an existing user and thus remove it from all user groups and replication groups where it was assigned	Write	user*		
				aws:ResourceTag/${TagKey}	
DeleteUserGroup	Grants permission to delete an existing user group	Write	usergroup*		
				aws:ResourceTag/${TagKey}	
DescribeCacheClusters	Grants permission to list information about provisioned cache clusters	List	cluster*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeCacheEngineVersions	Grants permission to list available cache engines and their versions	List			
DescribeCacheParameterGroups	Grants permission to list cache parameter group descriptions	List	parametergroup*		
				aws:ResourceTag/${TagKey}	
DescribeCacheParameters	Grants permission to retrieve the detailed parameter list for a particular cache parameter group	List	parametergroup*		
				aws:ResourceTag/${TagKey}	
DescribeCacheSecurityGroups	Grants permission to list cache security group descriptions	List	securitygroup*		
				aws:ResourceTag/${TagKey}	
DescribeCacheSubnetGroups	Grants permission to list cache subnet group descriptions	List	subnetgroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
DescribeEngineDefaultParameters	Grants permission to retrieve the default engine and system parameter information for the specified cache engine	List			
DescribeEvents	Grants permission to list events related to clusters, cache security groups, and cache parameter groups	List			
DescribeGlobalReplicationGroups	Grants permission to list information about global replication groups	List	globalreplicationgroup*		
DescribeReplicationGroups	Grants permission to list information about provisioned replication groups	List	replicationgroup*		
				aws:ResourceTag/${TagKey}	
DescribeReservedCacheNodes	Grants permission to list information about purchased reserved cache nodes	List	reserved-instance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
DescribeReservedCacheNodesOfferings	Grants permission to list available reserved cache node offerings	List			
DescribeServerlessCacheSnapshots	Grants permission to list information about serverless cache snapshots	List	serverlessscachesnapshot*	aws:ResourceTag/${TagKey}	
			serverlessscache	aws:ResourceTag/${TagKey}	
DescribeServerlessCaches	Grants permission to list serverless caches	List	serverlessscache*	aws:ResourceTag/${TagKey}	
DescribeServiceUpdates	Grants permission to list details of the service updates	List			
DescribeSnapshots	Grants permission to list information about cluster or replication group snapshots	List	snapshot*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
DescribeUpdateActions	Grants permission to list details of the update actions for a set of clusters or replication groups	List	cluster		
			replicationgroup		
				aws:ResourceTag/${TagKey}	
DescribeUserGroups	Grants permission to list information about Redis user groups	List	usergroup*		
				aws:ResourceTag/${TagKey}	
DescribeUsers	Grants permission to list information about Redis users	List	user*		
				aws:ResourceTag/${TagKey}	
DisassociateGlobalReplicationGroup	Grants permission to remove a secondary replication group from the global replication group	Write	globalreplicationgroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ExportServerlessCacheSnapshot	Grants permission to export a copy of a serverless cache at a specific moment in time to s3 bucket	Write	serverlessscachesnapshot*	aws:ResourceTag/${TagKey}	s3:DeleteObject s3:ListAllMyBuckets s3:PutObject
FailoverGlobalReplicationGroup	Grants permission to failover the primary region to a selected secondary region of a global replication group	Write	globalreplicationgroup*		
IncreaseNodeGroupsInGlobalReplicationGroup	Grants permission to increase the number of node groups in a global replication group	Write	globalreplicationgroup*		
				elasticache:NumNodeGroups	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
IncreaseReplicaCount	Grants permission to increase the number of replicas in a Redis (cluster mode disabled) replication group or the number of replica nodes in one or more node groups (shards) of a Redis (cluster mode enabled) replication group	Write	replicationgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey} elasticache:ReplicasPerNodeGroup	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
InterruptClusterAzPower [permission only]	Grants permission to test an AZ power interruption for an ElastiCache resource	Write	replicationgroup*		
				aws:ResourceTag/${TagKey}	
ListAllowedNodeTypeModifications	Grants permission to list available node type that can be used to scale a particular Redis cluster or replication group	List	cluster		
			replicationgroup		
				aws:ResourceTag/${TagKey}	
ListTagsForResource	Grants permission to list tags for an ElastiCache resource	Read	cluster		
			parametergroup		
			replicationgroup		
			reserved-instance		
			securitygroup		
			serverlesscache		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			serverlessscachesnapshot		
			snapshot		
			subnetgroup		
			user		
			usergroup		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyCacheCluster	Grants permission to modify settings for a cluster	Write	cluster*	elasticache:CacheNodeType elasticache:EngineVersion elasticache:MultiAZEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:CacheParameterGroupName	
			parametergroup		
			securitygroup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
ModifyCacheParameterGroup	Grants permission to modify parameters of a cache parameter group	Write	parametergroup*		
				aws:ResourceTag/${TagKey} elasticache:CacheParameterGroupName	
ModifyCacheSubnetGroup	Grants permission to modify an existing cache subnet group	Write	subnetgroup*		
				aws:ResourceTag/${TagKey}	
ModifyGlobalReplicationGroup	Grants permission to modify settings for a global replication group	Write	globalreplicationgroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				elasticache:CacheNodeType elasticache:EngineVersion elasticache:AutomaticFailoverEnabled	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyReplicationGroup	Grants permission to modify the settings for a replication group	Write	replicationgroup*	elasticache:CacheNodeType elasticache:EngineVersion elasticache:AutomaticFailoverEnabled elasticache:MultiAZEnabled elasticache:AuthTokenEnabled elasticache:SnapshotRetentionLimit elasticache:CacheParameterGroupName elasticache:Transi	ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tEncryptionEnabled elasticache:ClusterModeEnabled	
			parametergroup		
			securitygroup		
			usergroup		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyReplicationGroupShardConfiguration	Grants permission to add shards, remove shards, or rebalance the keyspaces among existing shards of a replication group	Write	replicationgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey} elasticache:NumNodeGroups	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyServerlessCache	Grants permission to modify parameters for a serverless cache	Write	serverlesscache*	aws:ResourceTag/${TagKey} elasticache:EngineVersion elasticache:SnapshotRetentionLimit elasticache:MinimumDataStorage elasticache:MaximumDataStorage elasticache:DataStorageUnit elasticache:MinimumECPUPerSecond	ec2:DescribeSecurityGroups ec2:DescribeTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				elasticache:MaximumECPUPerSecond	
			usergroup	aws:ResourceTag/${TagKey}	
ModifyUser	Grants permission to change Redis user password(s) and/or access string	Write	user*		
				aws:ResourceTag/${TagKey} elasticache:UserAuthenticationMode	
ModifyUserGroup	Grants permission to change list of users that belong to the user group	Write	user*		
			usergroup*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PurchaseReservedCacheNodesOffering	Grants permission to purchase a reserved cache node offering	Write	reserved-instance*		elasticache:AddTagsToResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
RebalanceSlotsInGlobalReplicationGroup	Grants permission to perform a key space rebalance operation to redistribute slots and ensure uniform key distribution across existing shards in a global replication group	Write	globalreplicationgroup*		
RebootCacheCluster	Grants permission to reboot some, or all, of the cache nodes within a provisioned cache cluster or replication group (cluster mode disabled)	Write	cluster*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RemoveTagsFromResource	Grants permission to remove tags from a ElastiCache resource	Tagging	cluster		
			parameter group		
			replicationgroup		
			reserved-instance		
			securitygroup		
			serverlesscache		
			serverlesscachesnapshot		
			snapshot		
			subnetgroup		
			user		
			usergroup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:ResourceTag/${TagKey}	
ResetCacheParameterGroup	Grants permission to modify parameters of a cache parameter group back to their default values	Write	parametergroup*		
				aws:ResourceTag/${TagKey} elasticache:CacheParameterGroupName	
RevokeCacheSecurityGroupIngress	Grants permission to remove an EC2 security group ingress from a ElastiCache security group	Write	securitygroup*		
				aws:ResourceTag/${TagKey}	
StartMigration	Grants permission to start a migration of data from hosted Redis on Amazon EC2 to ElastiCache for Redis	Write	replicationgroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
TestFailover	Grants permission to test automatic failover on a specified node group in a replication group	Write	replicationgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey}	
TestMigration	Grants permission to test a migration of data from hosted Redis on Amazon EC2 to ElastiCache for Redis	Write	replicationgroup*		

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

Resource types defined by Amazon ElastiCache

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
parameter group	`arn:${Partition}:elasticache:${Region}:${Account}:parametergroup:${CacheParameterGroupName}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:CacheParameterGroupName
securitygroup	`arn:${Partition}:elasticache:${Region}:${Account}:securitygroup:${CacheSecurityGroupName}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
		aws:TagKeys
subnetgroup	`arn:${Partition}:elasticache:${Region}:${Account}:subnetgroup:${CacheSubnetGroupName}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Resource types	ARN	Condition keys
replicationgroup	`arn:${Partition}:elasticache:${Region}:${Account}:replicationgroup:${ReplicationGroupId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:AtRestEncryptionEnabled elasticache:AuthTokenEnabled elasticache:AutomaticFailoverEnabled elasticache:CacheNodeType elasticache:CacheParameterGroupName elasticache:ClusterModeEnabled elasticache:EngineType elasticache:EngineVersion elasticache:KmsKeyId elasticache:MultiAZEnabled

Resource types	ARN	Condition keys
		elasticache:NumNodeGroups elasticache:ReplicasPerNodeGroup elasticache:SnapshotRetentionLimit elasticache:TransitEncryptionEnabled

Resource types	ARN	Condition keys
cluster	`arn:${Partition}:elasticache:${Region}:${Account}:cluster:${CacheClusterId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:AuthTokenEnabled elasticache:CacheNodeType elasticache:CacheParameterGroupName elasticache:EngineType elasticache:EngineVersion elasticache:MultiAZEnabled elasticache:SnapshotRetentionLimit
reserved-instance	`arn:${Partition}:elasticache:${Region}:${Account}:reserved-instance:${ReservedCacheNodeId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Resource types	ARN	Condition keys
snapshot	`arn:${Partition}:elasticache:${Region}:${Account}:snapshot:${SnapshotName}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:KmsKeyId

Resource types	ARN	Condition keys
globalreplicationgroup	`arn:${Partition}:elasticache::${Account}:globalreplicationgroup:${GlobalReplicationGroupId}`	elasticache:AtRestEncryptionEnabled elasticache:AuthTokenEnabled elasticache:AutomaticFailoverEnabled elasticache:CacheNodeType elasticache:CacheParameterGroupName elasticache:ClusterModeEnabled elasticache:EngineType elasticache:EngineVersion elasticache:KmsKeyId elasticache:MultiAZEnabled elasticache:NumNodeGroups elasticache:ReplicasPerNodeGroup elasticache:SnapshotRetentionLimit

Resource types	ARN	Condition keys
		elasticache:TransitEncryptionEnabled
user	`arn:${Partition}:elasticache:${Region}:${Account}:user:${UserId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:UserAuthenticationMode
usergroup	`arn:${Partition}:elasticache:${Region}:${Account}:usergroup:${UserGroupId}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys

Resource types	ARN	Condition keys
serverlesscache	`arn:${Partition}:elasticache:${Region}:${Account}:serverlesscache:${ServerlessCacheName}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:DataStorageUnit elasticache:EngineType elasticache:EngineVersion elasticache:KmsKeyId elasticache:MaximumDataStorage elasticache:MaximumECPUPerSecond elasticache:MinimumDataStorage elasticache:MinimumECPUPerSecond elasticache:SnapshotRetentionLimit

Resource types	ARN	Condition keys
serverlesscachesnapshot	`arn:${Partition}:elasticache:${Region}:${Account}:serverlesscachesnapshot:${ServerlessCacheSnapshotName}`	aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys elasticache:KmsKeyId

Condition keys for Amazon ElastiCache

Amazon ElastiCache 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 Amazon global condition context keys.

> **Note**
>
> To construct Condition elements using condition keys of String type, use the case insensitive condition operators StringEqualsIgnoreCase or StringNotEqualsIgnoreCase to compare a key to a string value.
> For information about conditions in an IAM policy to control access to ElastiCache, see ElastiCache Keys in the *Amazon ElastiCache User Guide*.

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

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters actions based on the tags associated with the resource	String
aws:TagKeys	Filters actions based on the tag keys that are passed in the request	ArrayOfString
elasticache:AtRestEncryptionEnabled	Filters access by the AtRestEncryptionEnabled parameter present in the request or default false value if parameter is not present	Bool
elasticache:AuthTokenEnabled	Filters access by the presence of non empty AuthToken parameter in the request	Bool
elasticache:AutomaticFailoverEnabled	Filters access by the AutomaticFailoverEnabled parameter in the request	Bool
elasticache:CacheNodeType	Filters access by the cacheNodeType parameter present in the request. This key can be used to restrict which cache node types can be used on cluster creation or scaling operations	String
elasticache:CacheParameterGroupName	Filters access by the CacheParameterGroupName parameter in the request	String
elasticache:ClusterModeEnabled	Filters access by the cluster mode parameter present in the request. Default value for single node group (shard) creations is false	Bool

Condition keys	Description	Type
elasticache:DataStorageUnit	Filters access by the CacheUsageLimits.DataStorage.Unit parameter in the CreateServerlessCache and ModifyServerlessCache request	String
elasticache:EngineType	Filters access by the engine type present in creation requests. For replication group creations, default engine 'redis' is used as key if parameter is not present	String
elasticache:EngineVersion	Filters access by the engineVersion parameter present in creation or cluster modification requests	String
elasticache:KmsKeyId	Filters access by the Key ID of the KMS key	String
elasticache:MaximumDataStorage	Filters access by the CacheUsageLimits.DataStorage.Maximum parameter in the CreateServerlessCache and ModifyServerlessCache request	Numeric
elasticache:MaximumECPUPerSecond	Filters access by the CacheUsageLimits.ECPUPerSecond.Maximum parameter in the CreateServerlessCache and ModifyServerlessCache request	Numeric
elasticache:MinimumDataStorage	Filters access by the CacheUsageLimits.DataStorage.Minimum parameter in the CreateServerlessCache and ModifyServerlessCache request	Numeric
elasticache:MinimumECPUPerSecond	Filters access by the CacheUsageLimits.ECPUPerSecond.Minimum parameter in the CreateServerlessCache and ModifyServerlessCache request	Numeric
elasticache:MultiAZEnabled	Filters access by the AZMode parameter, MultiAZEnabled parameter or the number of availability zones that the cluster or replication group can be placed in	Bool

Condition keys	Description	Type
elasticache:NumNodeGroups	Filters access by the NumNodeGroups or NodeGroupCount parameter specified in the request. This key can be used to restrict the number of node groups (shards) clusters can have after creation or scaling operations	Numeric
elasticache:ReplicasPerNodeGroup	Filters access by the number of replicas per node group (shards) specified in creations or scaling requests	Numeric
elasticache:SnapshotRetentionLimit	Filters access by the SnapshotRetentionLimit parameter in the request	Numeric
elasticache:TransitEncryptionEnabled	Filters access by the TransitEncryptionEnabled parameter present in the request. For replication group creations, default value 'false' is used as key if parameter is not present	Bool
elasticache:UserAuthenticationMode	Filters access by the UserAuthenticationMode parameter in the request	String

Actions, resources, and condition keys for Amazon Elemental MediaConvert

Amazon Elemental MediaConvert (service prefix: `mediaconvert`) 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 Elemental MediaConvert
- Resource types defined by Amazon Elemental MediaConvert
- Condition keys for Amazon Elemental MediaConvert

Actions defined by Amazon Elemental MediaConvert

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 Amazon. 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.

> **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 Certificate	Grants permission to associate an Amazon Certificate Manager (ACM) Amazon Resource Name (ARN) with Amazon Elemental MediaConvert	Write			
CancelJob	Grants permission to cancel an Amazon Elemental MediaConvert job that is waiting in queue	Write	Job*		
CreateJob	Grants permission to create and submit an Amazon Elemental MediaConvert job	Write	JobTemplate		
			Preset		
			Queue		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				mediaconvert:HttpInputsAllowed mediaconvert:HttpsInputsAllowed mediaconvert:S3InputsAllowed	
CreateJobTemplate	Grants permission to create an Amazon Elemental MediaConvert custom job template	Write	Preset		
			Queue		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePreset	Grants permission to create an Amazon Elemental MediaConvert custom output preset	Write		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateQueue	Grants permission to create an Amazon Elemental MediaConvert job queue	Write		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
DeleteJobTemplate	Grants permission to delete an Amazon Elemental MediaConvert custom job template	Write	JobTemplate*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeletePolicy	Grants permission to delete an Amazon Elemental MediaConvert policy	Write			
DeletePreset	Grants permission to delete an Amazon Elemental MediaConvert custom output preset	Write	Preset*		
DeleteQueue	Grants permission to delete an Amazon Elemental MediaConvert job queue	Write	Queue*		
DescribeEndpoints	Grants permission to subscribe to the Amazon Elemental MediaConvert service, by sending a request for an account-specific endpoint. All transcoding requests must be sent to the endpoint that the service returns	List			
DisassociateCertificate	Grants permission to remove an association between the Amazon Resource Name (ARN) of an Amazon Certificate Manager (ACM) certificate and an Amazon Elemental MediaConvert resource	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetJob	Grants permission to get an Amazon Elemental MediaConvert job	Read	Job*		
GetJobTemplate	Grants permission to get an Amazon Elemental MediaConvert job template	Read	JobTemplate*		
GetPolicy	Grants permission to get an Amazon Elemental MediaConvert policy	Read			
GetPreset	Grants permission to get an Amazon Elemental MediaConvert output preset	Read	Preset*		
GetQueue	Grants permission to get an Amazon Elemental MediaConvert job queue	Read	Queue*		
ListJobTemplates	Grants permission to list Amazon Elemental MediaConvert job templates	List			
ListJobs	Grants permission to list Amazon Elemental MediaConvert jobs	List	Queue		
ListPresets	Grants permission to list Amazon Elemental MediaConvert output presets	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListQueues	Grants permission to list Amazon Elemental MediaConvert job queues	List			
ListTagsForResource	Grants permission to retrieve the tags for a MediaConvert queue, preset, or job template	Read	Job		
			JobTemplate		
			Preset		
			Queue		
ListVersions	Grants permission to list Amazon Elemental MediaConvert job engine versions	List			
Probe	Grants permission to probe a file	Read			
PutPolicy	Grants permission to put an Amazon Elemental MediaConvert policy	Write			
SearchJobs	Grants permission to search Amazon Elemental MediaConvert jobs	List	Queue		
TagResource	Grants permission to add tags to a MediaConvert queue, preset, or job template	Tagging	Job		
			JobTemplate		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Preset		
			Queue		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from a MediaConvert queue, preset, or job template	Tagging	Job		
			JobTemplate		
			Preset		
			Queue		
				aws:TagKeys	
UpdateJobTemplate	Grants permission to update an Amazon Elemental MediaConvert custom job template	Write	JobTemplate*		
			Preset		
			Queue		
UpdatePreset	Grants permission to update an Amazon Elemental MediaConvert custom output preset	Write	Preset*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateQueue	Grants permission to update an Amazon Elemental MediaConvert job queue	Write	Queue*		

Resource types defined by Amazon Elemental MediaConvert

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
Job	`arn:${Partition}:mediaconvert:${Region}:${Account}:jobs/${JobId}`	aws:ResourceTag/${TagKey}
Queue	`arn:${Partition}:mediaconvert:${Region}:${Account}:queues/${QueueName}`	aws:ResourceTag/${TagKey}
Preset	`arn:${Partition}:mediaconvert:${Region}:${Account}:presets/${PresetName}`	aws:ResourceTag/${TagKey}
JobTemplate	`arn:${Partition}:mediaconvert:${Region}:${Account}:jobTemplates/${JobTemplateName}`	aws:ResourceTag/${TagKey}
CertificateAssociation	`arn:${Partition}:mediaconvert:${Region}:${Account}:certificates/${CertificateArn}`	

Condition keys for Amazon Elemental MediaConvert

Amazon Elemental MediaConvert 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 Amazon global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by tag keys in the request	ArrayOfString
mediaconvert:HttpInputsAllowed	Filters access by an HTTP input policy present in the account	Bool
mediaconvert:HttpsInputsAllowed	Filters access by an HTTPS input policy present in the account	Bool
mediaconvert:S3InputsAllowed	Filters access by an S3 input policy present in the account	Bool

Actions, resources, and condition keys for Amazon EMR Serverless

Amazon EMR Serverless (service prefix: `emr-serverless`) 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 EMR Serverless
- Resource types defined by Amazon EMR Serverless
- Condition keys for Amazon EMR Serverless

Actions defined by Amazon EMR Serverless

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 Amazon. 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.

> **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
AccessInteractiveEndpoints [permission only]	Grants permission to execute interactive workloads on an application	Write	application*		iam:PassRole
AccessLivyEndpoints [permission only]	Grants permission to execute interactive workloads on Livy Endpoint enabled on an EMR Serverless Application	Write	application*		iam:PassRole
CancelJobRun	Grants permission to cancel a job run	Write	jobRun*		
CreateApplication	Grants permission to create an Application	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteApplication	Grants permission to delete an application	Write	application*		
GetApplication	Grants permission to get application	Read	application*		
GetDashboardForJobRun	Grants permission to get job run dashboard	Read	jobRun*		
GetJobRun	Grants permission to get a job run	Read	jobRun*		
ListApplications	Grants permission to list applications	List			
ListJobRunAttempts	Grants permission to list job run attempts associated with a job run	List	jobRun*		
ListJobRuns	Grants permission to list job runs associated with an application	List	application*		
ListTagsForResource	Grants permission to list tags for the specified resource	Read	application		
			jobRun		
StartApplication	Grants permission to Start an application	Write	application*		
StartJobRun	Grants permission to start a job run	Write	application*		iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
StopApplication	Grants permission to Stop an application	Write	application*		
TagResource	Grants permission to tag the specified resource	Tagging	application		
			jobRun		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag the specified resource	Tagging	application		
			jobRun		
				aws:TagKeys	
UpdateApplication	Grants permission to Update an application	Write	application*		

Resource types defined by Amazon EMR Serverless

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:${Partition}:emr-serverless:${Region}:${Account}:/applications/${ApplicationId}`	aws:ResourceTag/${TagKey}
jobRun	`arn:${Partition}:emr-serverless:${Region}:${Account}:/applications/${ApplicationId}/jobruns/${JobRunId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon EMR Serverless

Amazon EMR Serverless 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 Amazon 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 the presence of tag keys in the request	ArrayOfString

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 Amazon. 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.

> **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*		
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 Amazon Web Services 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 Amazon Web Services 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 Amazon Web Services 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 Amazon 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 Amazon services. If a rule is created by an Amazon 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	String
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 Amazon service or Amazon 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 Fapiao Management

Amazon Fapiao Management (service prefix: `fapiao`) 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 Fapiao Management
- Resource types defined by Amazon Fapiao Management
- Condition keys for Amazon Fapiao Management

Actions defined by Amazon Fapiao 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 Amazon. 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.

> **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
GetAccountFapiaoSetting	Grants permission to get account fapiao setting	Read			
UpdateAccountFapiaoInformation	Grants permission to update account fapiao information	Write			

Resource types defined by Amazon Fapiao Management

Amazon Fapiao Management does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon Fapiao Management, specify `"Resource": "*"` in your policy.

Condition keys for Amazon Fapiao Management

Fapiao 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 Amazon global condition context keys.

Actions, resources, and condition keys for Amazon Free Tier

Amazon Free Tier (service prefix: `freetier`) 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 Free Tier
- Resource types defined by Amazon Free Tier
- Condition keys for Amazon Free Tier

Actions defined by Amazon Free Tier

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 Amazon. 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.

> **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
GetFreeTierAlertPreference [permission only]	Grants permission to get free tier alert preference (email address)	Read			
GetFreeTierUsage	Grants permission to get free tier usage limits and MTD usage status	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutFreeTierAlertPreference [permission only]	Grants permission to set free tier alert preference (email address)	Write			

Resource types defined by Amazon Free Tier

Amazon Free Tier does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon Free Tier, specify `"Resource": "*"` in your policy.

Condition keys for Amazon Free Tier

Free Tier 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 Amazon global condition context keys.

Actions, resources, and condition keys for Amazon FreeRTOS

Amazon FreeRTOS (service prefix: `freertos`) 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 FreeRTOS
- Resource types defined by Amazon FreeRTOS
- Condition keys for Amazon FreeRTOS

Actions defined by Amazon FreeRTOS

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 Amazon. 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.

> **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
CreateSoftwareConfiguration	Grants permission to create a software configuration	Write	configuration*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubscription	Grants permission to create a subscription for FreeRTOS extended maintenance plan (EMP)	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSoftwareConfiguration	Grants permission to delete the software configuration	Write	configuration*		
DescribeHardwarePlatform	Grants permission to describe the hardware platform	Read			
DescribeSoftwareConfiguration	Grants permission to describe the software configuration	Read	configuration*		
DescribeSubscription	Grants permission to describes the subscription	Read	subscription*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	for FreeRTOS extended maintenance plan (EMP)				
GetEmpPatchUrl	Grants permission to get URL for sotware patch-release, patch-diff and release notes under FreeRTOS extended maintenance plan (EMP)	Read			
GetSoftwareURL	Grants permission to get the URL for Amazon FreeRTOS software download	Read			
GetSoftwareURLForConfiguration	Grants permission to get the URL for Amazon FreeRTOS software download based on the configuration	Read			
GetSubscriptionBillingAmount	Grants permission to fetch the subscription billing amount for FreeRTOS extended maintenance plan (EMP)	Read			
ListFreeRTOSVersions	Grants permission to lists versions of AmazonFreeRTOS	List			
ListHardwarePlatforms	Grants permission to list the hardware platforms	List			
ListHardwareVendors	Grants permission to list the hardware vendors	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListSoftwareConfigurations	Grants permission to lists the software configurations	List			
ListSoftwarePatches	Grants permission to list software patches of subscription for FreeRTOS extended maintenance plan (EMP)	List			
ListSubscriptionEmails	Grants permission to list the subscription emails for FreeRTOS extended maintenance plan (EMP)	List			
ListSubscriptions	Grants permission to list the subscriptions for FreeRTOS extended maintenance plan (EMP)	List			
UpdateEmailRecipients	Grants permission to update list of subscription email address for FreeRTOS extended maintenance plan (EMP)	Write			
UpdateSoftwareConfiguration	Grants permission to update the software configuration	Write	configuration*		
VerifyEmail	Grants permission to verify the email for FreeRTOS extended maintenance plan (EMP)	Write			

Resource types defined by Amazon FreeRTOS

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	`arn:${Partition}:freertos:${Region}:${Account}:configuration/${ConfigurationName}`	aws:ResourceTag/${TagKey}
subscription	`arn:${Partition}:freertos:${Region}:${Account}:subscription/${SubscriptionID}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon FreeRTOS

Amazon FreeRTOS 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 Amazon global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by tag key present in the request that the user makes to Amazon FreeRTOS	String
aws:ResourceTag/${TagKey}	Filters access by tag key component attached to an Amazon FreeRTOS resource	String

Condition keys	Description	Type
aws:TagKeys	Filters access by the list of all the tag key names associated with the resource 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 Amazon. 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.

> **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*		
Associate FileSystemAliases	Grants permission to associate DNS 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
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*		
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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataRepositoryAssociation	Grants permission to create a new data respository association for an Amazon FSx for Lustre file system	Write	association*		fsx:TagResource
			file-system*		
				aws:RequestTag/${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]	Required to manage cross-account sharing of FSx volumes through Amazon 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 Amazon Web Services account in the Amazon Web Services Region of the endpoint that you're calling	Read			
DescribeDataRepositoryAssociations	Grants permission to return the descriptions of all data repository associations owned by your Amazon Web Services account in the Amazon Web Services Region of the endpoint that you're calling	Read			
DescribeDataRepositoryTasks	Grants permission to return the descriptions of all data repository tasks owned by your Amazon Web Services account in the Amazon Web Services Region of the endpoint that you're calling	Read			
DescribeFileCaches	Grants permission to return the descriptions of all file caches owned by your Amazon Web Services account in the Amazon Web Services 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 Amazon Web Services account in the Amazon Web Services Region of the endpoint that you're calling	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 Amazon Web Services account in the Amazon Web Services 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 Amazon Web Services account in the Amazon Web Services Region of the endpoint that you're calling	Read			
DescribeVolumes	Grants permission to return the descriptions of all volumes owned by your Amazon Web Services account in the Amazon Web Services Region of the endpoint that you're calling	Read			
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]	Required to manage cross-account sharing of FSx volumes through Amazon 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 Amazon Backup	Permissions management	backup*		
PutResourcePolicy [permission only]	Required to manage cross-account sharing of FSx volumes through Amazon 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*		
TagResource	Grants permission to tag an Amazon FSx resource	Tagging	association		
			backup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			file-cache		
			file-system		
			snapshot		
			storage-virtual-machine		
			task		
			volume		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove a tag from an Amazon FSx resource	Tagging	association		
			backup		
			file-cache		
			file-system		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot		
			storage-virtual-machine		
			task		
			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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateVolume	Grants permission to update volume configuration	Write	volume*		
				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}

Resource types	ARN	Condition keys
backup	arn:${Partition}:fsx:${Region}:${Account}:backup/${BackupId}	aws:ResourceTag/${TagKey}
storage-virtual-machine	arn:${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 Amazon 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
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 Amazon GameLift

Amazon GameLift (service prefix: `gamelift`) 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 GameLift
- Resource types defined by Amazon GameLift
- Condition keys for Amazon GameLift

Actions defined by Amazon GameLift

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 Amazon. 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.

> **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
AcceptMatch	Grants permission to register player acceptance or rejection of a proposed FlexMatch match	Write			
ClaimGameServer	Grants permission to locate and reserve a game server to host a new game session	Write	gameServerGroup*		
CreateAlias	Grants permission to define a new alias for a fleet	Write		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateBuild	Grants permission to create a new game build using files stored in an Amazon S3 bucket	Write		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource iam:PassRole s3:GetObject
CreateContainerFleet	Grants permission to create a new container fleet of computing resources to run your game servers	Write		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeAvailabilityZones ec2:DescribeRegions gamelift:TagResource iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateContainerGroupDefinition	Grants permission to create a new container group definition using images stored in an Amazon ECR repository	Write		aws:RequestTag/${TagKey} aws:TagKeys	ecr:BatchGetImage ecr:DescribeImages ecr:GetAuthorizationToken ecr:GetDownloadUrlForLayer gamelift:TagResource
CreateFleet	Grants permission to create a new fleet of computing resources to run your game servers	Write		aws:RequestTag/${TagKey} aws:TagKeys	ec2:DescribeAvailabilityZones ec2:DescribeRegions gamelift:TagResource iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateFleetLocations	Grants permission to specify additional locations for a fleet	Write	container Fleet		ec2:DescribeAvailabilityZones ec2:DescribeRegions
			fleet		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateGameServerGroup	Grants permission to create a new game server group, set up a corresponding Auto Scaling group, and launche instances to host game servers	Write		aws:RequestTag/${TagKey} aws:TagKeys	autoscaling:CreateAutoScalingGroup autoscaling:DescribeAutoScalingGroups autoscaling:PutLifecycleHook autoscaling:PutScalingPolicy ec2:DescribeAvailabilityZones ec2:DescribeSubnets events:PutRule

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					events:PutTargets gamelift:TagResource iam:PassRole
CreateGameSession	Grants permission to start a new game session on a specified fleet	Write			
CreateGameSessionQueue	Grants permission to set up a new queue for processing game session placement requests	Write		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource
CreateLocation	Grants permission to define a new location for a fleet	Write		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateMatchmakingConfiguration	Grants permission to create a new FlexMatch matchmaker	Write		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource
CreateMatchmakingRuleSet	Grants permission to create a new matchmaking rule set for FlexMatch	Write		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource
CreatePlayerSession	Grants permission to reserve an available game session slot for a player	Write			
CreatePlayerSessions	Grants permission to reserve available game session slots for multiple players	Write			
CreateScript	Grants permission to create a new Realtime Servers script	Write		aws:RequestTag/${TagKey} aws:TagKeys	gamelift:TagResource iam:PassRole s3:GetObject

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateVpcPeeringAuthorization	Grants permission to allow GameLift to create or delete a peering connection between a GameLift fleet VPC and a VPC on another Amazon Web Services account	Write			ec2:AcceptVpcPeeringConnection ec2:AuthorizeSecurityGroupEgress ec2:AuthorizeSecurityGroupIngress ec2:CreateRoute ec2:DeleteRoute ec2:DescribeRouteTables ec2:DescribeSecurityGroups ec2:RevokeSecurityGroupEgress

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:RevokeSecurityGroupIngress
CreateVpcPeeringConnection	Grants permission to establish a peering connection between your GameLift fleet VPC and a VPC on another account	Write			
DeleteAlias	Grants permission to delete an alias	Write	alias*		
DeleteBuild	Grants permission to delete a game build	Write	build*		
DeleteContainerFleet	Grants permission to delete a container fleet	Write	containerFleet*		
DeleteContainerGroupDefinition	Grants permission to delete a container group definition	Write	containerGroupDefinition*		
DeleteFleet	Grants permission to delete an empty fleet	Write	fleet*		
DeleteFleetLocations	Grants permission to delete locations for a fleet	Write	containerFleet		
			fleet		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteGameServerGroup	Grants permission to permanently delete a game server group and terminate FleetIQ activity for the corresponding Auto Scaling group	Write	gameServerGroup*		autoscaling:DeleteAutoScalingGroup autoscaling:DescribeAutoScalingGroups autoscaling:ExitStandby autoscaling:ResumeProcesses autoscaling:SetInstanceProtection autoscaling:UpdateAutoScalingGroup
DeleteGameSessionQueue	Grants permission to delete an existing game session queue	Write	gameSessionQueue*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteLocation	Grants permission to delete a location	Write	location*		
DeleteMatchmakingConfiguration	Grants permission to delete an existing FlexMatch matchmaker	Write	matchmakingConfiguration*		
DeleteMatchmakingRuleSet	Grants permission to delete an existing FlexMatch matchmaking rule set	Write	matchmakingRuleSet*		
DeleteScalingPolicy	Grants permission to delete a set of auto-scaling rules	Write	containerFleet		
			fleet		
DeleteScript	Grants permission to delete a Realtime Servers script	Write	script*		
DeleteVpcPeeringAuthorization	Grants permission to cancel a VPC peering authorization	Write			
DeleteVpcPeeringConnection	Grants permission to remove a peering connection between VPCs	Write			
DeregisterCompute	Grants permission to deregister a compute against a fleet	Write	fleet*		
DeregisterGameServer	Grants permission to remove a game server from a game server group	Write	gameServerGroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeAlias	Grants permission to retrieve properties for an alias	Read	alias*		
DescribeBuild	Grants permission to retrieve properties for a game build	Read	build*		
DescribeCompute	Grants permission to retrieve information for a compute in a fleet	Read	containerFleet		
			fleet		
DescribeContainerFleet	Grants permission to retrieve the properties of an existing container fleet	Read	containerFleet*		
DescribeContainerGroupDefinition	Grants permission to retrieve the properties of an existing container group definition	Read	containerGroupDefinition*		
DescribeEC2InstanceLimits	Grants permission to retrieve the maximum allowed and current usage for EC2 instance types	Read			
DescribeFleetAttributes	Grants permission to retrieve general properties, including status, for fleets	Read			
DescribeFleetCapacity	Grants permission to retrieve the current capacity settings for managed fleets	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeFleetDeployment	Grants permission to retrieve the properties of an existing fleet deployment	Read	containerFleet*		
DescribeFleetEvents	Grants permission to retrieve entries from a fleet's event log	Read	containerFleet		
			fleet		
DescribeFleetLocationAttributes	Grants permission to retrieve general properties, including statuses, for a fleet's locations	Read	containerFleet		
			fleet		
DescribeFleetLocationCapacity	Grants permission to retrieve the current capacity setting for a fleet's location	Read	containerFleet		
			fleet		
DescribeFleetLocationUtilization	Grants permission to retrieve utilization statistics for fleet's location	Read	fleet*		
DescribeFleetPortSettings	Grants permission to retrieve the inbound connection permissions for a fleet	Read	fleet*		
DescribeFleetUtilization	Grants permission to retrieve utilization statistics for fleets	Read			
DescribeGameServer	Grants permission to retrieve properties for a game server	Read	gameServerGroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeGameServerGroup	Grants permission to retrieve properties for a game server group	Read	gameServerGroup*		
DescribeGameServerInstances	Grants permission to retrieve the status of EC2 instances in a game server group	Read	gameServerGroup*		
DescribeGameSessionDetails	Grants permission to retrieve properties for game sessions in a fleet, including the protection policy	Read			
DescribeGameSessionPlacement	Grants permission to retrieve details of a game session placement request	Read			
DescribeGameSessionQueues	Grants permission to retrieve properties for game session queues	Read			
DescribeGameSessions	Grants permission to retrieve properties for game sessions in a fleet	Read			
DescribeInstances	Grants permission to retrieve information about instances in a managed fleet	Read	containerFleet		
			fleet		
DescribeMatchmaking	Grants permission to retrieve details of matchmaking tickets	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeMatchmakingConfigurations	Grants permission to retrieve properties for FlexMatch matchmakers	Read			
DescribeMatchmakingRuleSets	Grants permission to retrieve properties for FlexMatch matchmaking rule sets	Read			
DescribePlayerSessions	Grants permission to retrieve properties for player sessions in a game session	Read			
DescribeRuntimeConfiguration	Grants permission to retrieve the current runtime configuration for a fleet	Read	fleet*		
DescribeScalingPolicies	Grants permission to retrieve all scaling policies that are applied to a fleet	Read	containerFleet		
			fleet		
DescribeScript	Grants permission to retrieve properties for a Realtime Servers script	Read	script*		
DescribeVpcPeeringAuthorizations	Grants permission to retrieve valid VPC peering authorizations	Read			
DescribeVpcPeeringConnections	Grants permission to retrieve details on active or pending VPC peering connections	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetComputeAccess	Grants permission to retrieve credentials to remotely access a compute in a managed fleet	Read	containerFleet		
			fleet		
GetComputeAuthToken	Grants permission to retrieve an authentication token that allows processes on a compute to send requests to the Amazon GameLift service	Read	containerFleet		
			fleet		
GetGameSessionLogUrl	Grants permission to retrieve the location of stored logs for a game session	Read			
GetInstanceAccess	Grants permission to request remote access to a specified fleet instance	Read	fleet*		
ListAliases	Grants permission to retrieve all aliases that are defined in the current Region	List			
ListBuilds	Grants permission to retrieve all game build in the current Region	List			
ListCompute	Grants permission to retrieve all compute resources in the current Region	List	containerFleet		
			fleet		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListContainerFleets	Grants permission to retrieve the properties of all existing container fleets in the current Region	List			
ListContainerGroupDefinitionVersions	Grants permission to retrieve the properties of all versions of an existing container group definition	List	containerGroupDefinition*		
ListContainerGroupDefinitions	Grants permission to retrieve the properties of all existing container group definitions in the current Region	List			
ListFleetDeployments	Grants permission to retrieve the properties of all existing fleet deployments in the current Region	List			
ListFleets	Grants permission to retrieve a list of fleet IDs for all fleets in the current Region	List			
ListGameServerGroups	Grants permission to retrieve all game server groups that are defined in the current Region	List			
ListGameServers	Grants permission to retrieve all game servers that are currently running in a game server group	List	gameServerGroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListLocations	Grants permission to retrieve all locations in this account	List			
ListScripts	Grants permission to retrieve properties for all Realtime Servers scripts in the current region	List			
ListTagsForResource	Grants permission to retrieve tags for GameLift resources	Read	alias		
			build		
			containerFleet		
			containerGroupDefinition		
			fleet		
			gameServerGroup		
			gameSessionQueue		
			location		
			matchmakingConfiguration		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			matchmakingRuleSet		
			script		
PutScalingPolicy	Grants permission to create or update a fleet auto-scaling policy	Write	containerFleet		
			fleet		
RegisterCompute	Grants permission to register a compute against a fleet	Write	fleet*		
RegisterGameServer	Grants permission to notify GameLift FleetIQ when a new game server is ready to host gameplay	Write	gameServerGroup*		
RequestUploadCredentials	Grants permission to retrieve fresh upload credentials to use when uploading a new game build	Read	build*		
ResolveAlias	Grants permission to retrieve the fleet ID associated with an alias	Read	alias*		
ResumeGameServerGroup	Grants permission to reinstate suspended FleetIQ activity for a game server group	Write	gameServerGroup*		
SearchGameSessions	Grants permission to retrieve game sessions that match a set of search criteria	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartFleetActions	Grants permission to resume auto-scaling activity on a fleet after it was suspended with StopFleetActions()	Write	containerFleet		
			fleet		
StartGameSessionPlacement	Grants permission to send a game session placement request to a game session queue	Write	gameSessionQueue*		
StartMatchBackfill	Grants permission to request FlexMatch matchmaking to fill available player slots in an existing game session	Write			
StartMatchmaking	Grants permission to request FlexMatch matchmaking for one or a group of players and initiate game session placement	Write			
StopFleetActions	Grants permission to suspend auto-scaling activity on a fleet	Write	containerFleet		
			fleet		
StopGameSessionPlacement	Grants permission to cancel a game session placement request that is in progress	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopMatchmaking	Grants permission to cancel a matchmaking or match backfill request that is in progress	Write			
SuspendGameServerGroup	Grants permission to temporarily stop FleetIQ activity for a game server group	Write	gameServerGroup*		
TagResource	Grants permission to tag GameLift resources	Tagging	alias		
			build		
			containerFleet		
			containerGroupDefinition		
			fleet		
			gameServerGroup		
			gameSessionQueue		
			location		
			matchmakingConfiguration		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			matchmakingRuleSet		
			script		
				aws:RequestTag/${TagKey} aws:TagKeys	
Terminate GameSession	Grants permission to shut down an existing game session	Write			
UntagResource	Grants permission to untag GameLift resources	Tagging	alias		
			build		
			containerFleet		
			containerGroupDefinition		
			fleet		
			gameServerGroup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			gameSessionQueue		
			location		
			matchmakingConfiguration		
			matchmakingRuleSet		
			script		
				aws:TagKeys	
UpdateAlias	Grants permission to update the properties of an existing alias	Write	alias*		
UpdateBuild	Grants permission to update an existing build's metadata	Write	build*		
UpdateContainerFleet	Grants permission to update an existing container fleet	Write	containerFleet*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateContainerGroupDefinition	Grants permission to update the properties of an existing container group definition	Write	containerGroupDefinition*		ecr:BatchGetImage ecr:DescribeImages ecr:GetAuthorizationToken ecr:GetDownloadUrlForLayer
UpdateFleetAttributes	Grants permission to update the general properties of an existing fleet	Write	fleet*		
UpdateFleetCapacity	Grants permission to adjust a managed fleet's capacity settings	Write	containerFleet		
			fleet		
UpdateFleetPortSettings	Grants permission to adjust a fleet's port settings	Write	fleet*		
UpdateGameServer	Grants permission to change game server properties, health status, or utilization status	Write	gameServerGroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateGameServerGroup	Grants permission to update properties for game server group, including allowed instance types	Write	gameServerGroup*		iam:PassRole
UpdateGameSession	Grants permission to update the properties of an existing game session	Write			
UpdateGameSessionQueue	Grants permission to update properties of an existing game session queue	Write	gameSessionQueue*		
UpdateMatchmakingConfiguration	Grants permission to update properties of an existing FlexMatch matchmaking configuration	Write	matchmakingConfiguration*		
UpdateRuntimeConfiguration	Grants permission to update how server processes are configured on instances in an existing fleet	Write	fleet*		
UpdateScript	Grants permission to update the metadata and content of an existing Realtime Servers script	Write	script*		iam:PassRole s3:GetObject
ValidateMatchmakingRuleSet	Grants permission to validate the syntax of a FlexMatch matchmaking rule set	Read			

Resource types defined by Amazon GameLift

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:${Partition}:gamelift:${Region}::alias/${AliasId}`	aws:ResourceTag/${TagKey}
build	`arn:${Partition}:gamelift:${Region}:${Account}:build/${BuildId}`	aws:ResourceTag/${TagKey}
containerGroupDefinition	`arn:${Partition}:gamelift:${Region}:${Account}:containergroupdefinition/${Name}`	aws:ResourceTag/${TagKey}
containerFleet	`arn:${Partition}:gamelift:${Region}:${Account}:containerfleet/${FleetId}`	aws:ResourceTag/${TagKey}
fleet	`arn:${Partition}:gamelift:${Region}:${Account}:fleet/${FleetId}`	aws:ResourceTag/${TagKey}
gameServerGroup	`arn:${Partition}:gamelift:${Region}:${Account}:gameservergroup/${GameServerGroupName}`	aws:ResourceTag/${TagKey}
gameSessionQueue	`arn:${Partition}:gamelift:${Region}:${Account}:gamesessionqueue/${GameSessionQueueName}`	aws:ResourceTag/${TagKey}
location	`arn:${Partition}:gamelift:${Region}:${Account}:location/${LocationId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
matchmakingConfiguration	`arn:${Partition}:gamelift:${Region}:${Account}:matchmakingconfiguration/${MatchmakingConfigurationName}`	aws:ResourceTag/${TagKey}
matchmakingRuleSet	`arn:${Partition}:gamelift:${Region}:${Account}:matchmakingruleset/${MatchmakingRuleSetName}`	aws:ResourceTag/${TagKey}
script	`arn:${Partition}:gamelift:${Region}:${Account}:script/${ScriptId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon GameLift

Amazon GameLift 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 Amazon 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 Glue

Amazon Glue (service prefix: `glue`) 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 Glue
- Resource types defined by Amazon Glue
- Condition keys for Amazon Glue

Actions defined by Amazon Glue

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 Amazon. 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.

> **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
AuthorizeInboundIntegration [permission only]	Grants permission to Glue to continuously validate that the target Arn can receive data replicated from the source ARN	Write	integration*		
BatchCreatePartition	Grants permission to create one or more partitions	Write	database*		
			rootcatalog*		
			table*		
			catalog		
BatchDeleteConnection	Grants permission to delete one or more connections	Write	connection*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			rootcatalog*		
BatchDeletePartition	Grants permission to delete one or more partitions	Write	database*		
			rootcatalog*		
			table*		
			catalog		
BatchDeleteTable	Grants permission to delete one or more tables	Write	database*		
			rootcatalog*		
			table*		
			catalog		
BatchDeleteTableVersion	Grants permission to delete one or more versions of a table	Write	database*		
			rootcatalog*		
			table*		
			catalog		
BatchGetBlueprints	Grants permission to retrieve one or more blueprints	Read	blueprint*		
BatchGetCrawlers	Grants permission to retrieve one or more crawlers	Read	crawler*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetCustomEntityTypes	Grants permission to retrieve one or more Custom Entity Types	Read			
BatchGetDevEndpoints	Grants permission to retrieve one or more development endpoints	Read	devendpoint*		
BatchGetJobs	Grants permission to retrieve one or more jobs	Read	job*		
BatchGetPartition	Grants permission to retrieve one or more partitions	Read	database*		
			rootcatalog*		
			table*		
			catalog		
BatchGetStageFiles	Grants permission to batch get stage files for SparkUI	Permissions management			
BatchGetTableOptimizer	Grants permission to return the configuration for the specified table optimizers	Read	database*		glue:GetTable
			rootcatalog*		
			table*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetTriggers	Grants permission to retrieve one or more triggers	Read	trigger*		
BatchGetWorkflows	Grants permission to retrieve one or more workflows	Read	workflow*		
BatchStopJobRun	Grants permission to stop one or more job runs for a job	Write	job*		
BatchUpdatePartition	Grants permission to update one or more partitions	Write	database*		
			rootcatalog*		
			table*		
			catalog		
CancelDataQualityRuleRecommendationRun	Grants permission to stop a running Data Quality rule recommendation run	Write	dataQualityRuleset*		
CancelDataQualityRulesetEvaluationRun	Grants permission to stop a running Data Quality ruleset evaluation run	Write	dataQualityRuleset*		
CancelMLTaskRun	Grants permission to stop a running ML Task Run	Write	mlTransform*		
CancelStatement	Grants permission to cancel a statement in an interactive session	Write	session*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CheckSchemaVersionValidity	Grants permission to retrieve a check the validity of schema version	Read			
CreateBlueprint	Grants permission to create a blueprint	Write	blueprint*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCatalog	Grants permission to create a catalog	Write	catalog*		
			rootcatalog*		
CreateClassifier	Grants permission to create a classifier	Write			
CreateColumnStatisticsTaskSettings	Grants permission to create settings for a column statistics task	Write	database*		
			rootcatalog*		
			table*		
CreateConnection	Grants permission to create a connection	Write	rootcatalog*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCrawler	Grants permission to create a crawler	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomEntityType	Grants permission to create a Custom Entity Type	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataQualityRuleset	Grants permission to create a Data Quality ruleset	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDatabase	Grants permission to create a database	Write	database*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			rootcatalog*		
			catalog		
CreateDevEndpoint	Grants permission to create a development endpoint	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateInboundIntegration [permission only]	Grants permission to the source principal to create an inbound integration for data to be replicated from the source into the target	Write			
CreateIntegration	Grants permission to create an integration	Write	catalog*		kms:CreateGrant kms:DescribeKey
			connection*		
			database*		
			integration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateIntegrationResourceProperty	Grants permission to create integration resource property	Write	catalog*		
			connection*		
			database*		
CreateIntegrationTableProperties	Grants permission to create integration table properties	Write	catalog*		
			connection*		
			database*		
CreateJob	Grants permission to create a job	Write	job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys glue:VpcIds glue:SubnetIds glue:SecurityGroupIds	
CreateMLTransform	Grants permission to create an ML Transform	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePartition	Grants permission to create a partition	Write	database*		
			rootcatalog*		
			table*		
			catalog		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePartitionIndex	Grants permission to create a specified partition index in an existing table	Write	database*		
			rootcatalog*		
			table*		
			catalog		
CreateRegistry	Grants permission to create a new schema registry	Write	registry*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSchema	Grants permission to create a new schema container	Write	registry*		
			schema*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateScript	Grants permission to create a script	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSecurityConfiguration	Grants permission to create a security configuration	Write			
CreateSession	Grants permission to create an interactive session	Write	session*		
				aws:RequestTag/${TagKey} aws:TagKeys glue:VpcIds glue:SubnetIds glue:SecurityGroupIds	
CreateTable	Grants permission to create a table	Write	database*		
			rootcatalog*		
			table*		
			catalog		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTableOptimizer	Grants permission to create a new table optimizer for a specific function. Compaction is the only currently supported optimizer type	Write	database*		glue:GetTable
			rootcatalog*		
			table*		
CreateTrigger	Grants permission to create a trigger	Write	trigger*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUsageProfile	Grants permission to create a usage profile	Write	usageProfile*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUserDefinedFunction	Grants permission to create a function definition	Write	database*		
			rootcatalog*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			catalog		
CreateWorkflow	Grants permission to create a workflow	Write	workflow*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteBlueprint	Grants permission to delete a blueprint	Write	blueprint*		
DeleteCatalog	Grants permission to delete a catalog	Write	rootcatalog*		
			catalog		
DeleteClassifier	Grants permission to delete a classifier	Write			
DeleteColumnStatisticsForPartition	Grants permission to delete the partition column statistics of a column	Write	database*		
			rootcatalog*		
			table*		
			catalog		
DeleteColumnStatisticsForTable	Grants permission to delete the table statistics of columns	Write	database*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			rootcatalog*		
			table*		
			catalog		
DeleteColumnStatisticsTaskSettings	Grants permission to delete settings for a column statistics task	Write	database*		
			rootcatalog*		
			table*		
DeleteConnection	Grants permission to delete a connection	Write	connection*		
			rootcatalog*		
DeleteCrawler	Grants permission to delete a crawler	Write	crawler*		
DeleteCustomEntityType	Grants permission to delete a Custom Entity Type	Write			
DeleteDataQualityRuleset	Grants permission to delete a Data Quality ruleset	Write	dataQualityRuleset*		
DeleteDatabase	Grants permission to delete a database	Write	database*		
			rootcatalog*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			table*		
			userdefinedfunction*		
			catalog		
DeleteDevEndpoint	Grants permission to delete a development endpoint	Write	devendpoint*		
DeleteIntegration	Grants permission to delete an integration	Write	integration*		
				aws:ResourceTag/${TagKey}	
DeleteIntegrationTableProperties	Grants permission to delete integration table properties	Write	catalog*		
			connection*		
			database*		
DeleteJob	Grants permission to delete a job	Write	job*		
DeleteMLTransform	Grants permission to delete an ML Transform	Write	mlTransform*		
DeletePartition	Grants permission to delete a partition	Write	database*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			rootcatalog*		
			table*		
			catalog		
DeletePartitionIndex	Grants permission to delete a specified partition index from an existing table	Write	database*		
			rootcatalog*		
			table*		
			catalog		
DeleteRegistry	Grants permission to delete a schema registry	Write	registry*		
DeleteResourcePolicy	Grants permission to delete a resource policy	Permissions management	rootcatalog*		
DeleteSchema	Grants permission to delete a schema container	Write	registry*		
			schema*		
DeleteSchemaVersions	Grants permission to delete a range of schema versions	Write	registry*		
			schema*		
DeleteSecurityConfiguration	Grants permission to delete a security configuration	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteSession	Grants permission to delete an interactive session after stopping the session if not already stopped	Write	session*		
DeleteTable	Grants permission to delete a table	Write	database*		
			rootcatalog*		
			table*		
			catalog		
DeleteTableOptimizer	Grants permission to delete an optimizer and all associated metadata for a table. The optimization will no longer be performed on the table	Write	database*		glue:GetTable
			rootcatalog*		
			table*		
DeleteTableVersion	Grants permission to delete a version of a table	Write	database*		
			rootcatalog*		
			table*		
			catalog		
DeleteTrigger	Grants permission to delete a trigger	Write	trigger*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteUsageProfile	Grants permission to delete a usage profile	Write	usageProfile*		
DeleteUserDefinedFunction	Grants permission to delete a function definition	Write	database*		
			rootcatalog*		
			userdefinedfunction*		
			catalog		
DeleteWorkflow	Grants permission to delete a workflow	Write	workflow*		
DeregisterDataPreview	Grants permission to terminate Glue Studio Notebook session	Permissions management			
DescribeConnectionType	Grants permission to describe connection type in glue studio	Permissions management			
DescribeEntity	Grants permission to describe entity in glue studio	Permissions management	connection*		
			rootcatalog*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeInboundIntegrations	Grants permission to list the inbound integrations	List			
DescribeIntegrations	Grants permission to describe zero-ETL integrations	List	integration*		
				aws:ResourceTag/${TagKey}	
GetBlueprint	Grants permission to retrieve a blueprint	Read	blueprint*		
GetBlueprintRun	Grants permission to retrieve a blueprint run	Read	blueprint*		
GetBlueprintRuns	Grants permission to retrieve all runs of a blueprint	Read	blueprint*		
GetCatalog	Grants permission to retrieve a catalog	Read	rootcatalog*		
			catalog		
				glue:EnabledForRedshiftAutoDiscovery	
GetCatalogImportStatus	Grants permission to retrieve the catalog import status	Read	rootcatalog*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCatalogs	Grants permission to retrieve all catalogs	Read	rootcatalog*		
			catalog		
				glue:EnabledForRedshiftAutoDiscovery	
GetClassifier	Grants permission to retrieve a classifier	Read			
GetClassifiers	Grants permission to list all classifiers	Read			
GetColumnStatisticsForPartition	Grants permission to retrieve partition statistics of columns	Read	database*		
			rootcatalog*		
			table*		
			catalog		
GetColumnStatisticsForTable	Grants permission to retrieve table statistics of columns	Read	database*		
			rootcatalog*		
			table*		
			catalog		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetColumnStatisticsTaskRun	Grants permission to retrieve Column Statistics run information for the table based on run-id	Read			
GetColumnStatisticsTaskRuns	Grants permission to retrieve Column Statistics run information for the table based on run-ids	Read			
GetColumnStatisticsTaskSettings	Grants permission to retrieve settings for a column statistics task	Read			
GetCompletion	Grants permission to get generated response for a completion request in Glue from Amazon Q	Read	completion*		
GetConnection	Grants permission to retrieve a connection	Read	connection*		
			rootcatalog*		
GetConnections	Grants permission to retrieve a list of connections	Read	connection*		
			rootcatalog*		
GetCrawler	Grants permission to retrieve a crawler	Read	crawler*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCrawlerMetrics	Grants permission to retrieve metrics about crawlers	Read			
GetCrawlers	Grants permission to retrieve all crawlers	Read			
GetCustomEntityType	Grants permission to read a Custom Entity Type	Read			
GetDashboardUrl	Grants permission to generate presigned url for accessing spark live UI	Read	session*		
GetDataCatalogEncryptionSettings	Grants permission to retrieve catalog encryption settings	Read	rootcatalog*		
GetDataPreviewStatement	Grants permission to get Data Preview Statement	Permissions management			
GetDataQualityModel	Grants permission to retrieve the training status of the prediction model for a statistic	Read	dataQualityRuleset*		
			job*		
GetDataQualityModelResult	Grants permission to retrieve the predictions for a statistic from the latest model	Read	dataQualityRuleset*		
			job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDataQualityResult	Grants permission to retrieve a Data Quality result	Read	dataQualityRuleset*		
GetDataQualityRuleRecommendationRun	Grants permission to retrieve a Data Quality rule recommendation run	Read	dataQualityRuleset*		
GetDataQualityRuleset	Grants permission to retrieve a Data Quality ruleset	Read	dataQualityRuleset*		
GetDataQualityRulesetEvaluationRun	Grants permission to retrieve a Data Quality rule recommendation run	Read	dataQualityRuleset*		
GetDatabase	Grants permission to retrieve a database	Read	database*		
			rootcatalog*		
			catalog		
GetDatabases	Grants permission to retrieve all databases	Read	database*		
			rootcatalog*		
			catalog		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDataflowGraph	Grants permission to transform a script into a directed acyclic graph (DAG)	Read			
GetDevEndpoint	Grants permission to retrieve a development endpoint	Read	devendpoint*		
GetDevEndpoints	Grants permission to retrieve all development endpoints	Read			
GetEntityRecords	Grants permission to preview entity records in glue	Read	catalog*		
			connection		
GetEnvironment	Grants permission to get environment details for SparkUI	Permissions management			
GetExecutors	Grants permission to get executors for SparkUI	Permissions management			
GetExecutorsThreads	Grants permission to get executor threads for SparkUI	Permissions management			
GetGeneratedCode	Transforms a directed acyclic graph (DAG) into code	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetIntegrationResourceProperty	Grants permission to retrieve the integration resource property	Read	catalog*		
			connection*		
			database*		
GetIntegrationTableProperties	Grants permission to retrieve the integration table properties	Read	catalog*		
			connection*		
			database*		
GetJob	Grants permission to retrieve a job	Read	job*		
GetJobBookmark	Grants permission to retrieve a job bookmark	Read			
GetJobRun	Grants permission to retrieve a job run	Read	job*		
GetJobRuns	Grants permission to retrieve all job runs of a job	Read	job*		
GetJobUpgradeAnalysis	Grants permission to retrieve an upgrade analysis for a job	Read	job*		
GetJobs	Grants permission to retrieve all current jobs	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetLogParsingStatus	Grants permission to get log parsing status for SparkUI	Permissions management			
GetMLTaskRun	Grants permission to retrieve an ML Task Run	Read	mlTransform*		
GetMLTaskRuns	Grants permission to retrieve all ML Task Runs	List	mlTransform*		
GetMLTransform	Grants permission to retrieve an ML Transform	Read	mlTransform*		
GetMLTransforms	Grants permission to retrieve all ML Transforms	List	mlTransform*		
GetMapping	Grants permission to create a mapping	Read			
GetNotebookInstanceStatus	Grants permission to retrieve Glue Studio Notebooks session status	Permissions management			
GetPartition	Grants permission to retrieve a partition	Read	database*		
			rootcatalog*		
			table*		
			catalog		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetPartitionIndexes	Grants permission to retrieve partition indexes for a table	Read	database*		
			rootcatalog*		
			table*		
			catalog		
GetPartitions	Grants permission to retrieve the partitions of a table	Read	database*		
			rootcatalog*		
			table*		
			catalog		
GetPlan	Grants permission to retrieve a mapping for a script	Read			
GetQueries	Grants permission to get queries for SparkUI	Permissions management			
GetQuery	Grants permission to get a specific query for SparkUI	Permissions management			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRecipeAction	Grants permission to get the result of a Data Preparation Recipe statement	Permissions management			
GetRegistry	Grants permission to retrieve a schema registry	Read	registry*		
GetResourcePolicies	Grants permission to retrieve resource policies	Read	rootcatalog*		
GetResourcePolicy	Grants permission to retrieve a resource policy	Read	rootcatalog*		
GetSchema	Grants permission to retrieve a schema container	Read	registry*		
			schema*		
GetSchemaByDefinition	Grants permission to retrieve a schema version based on schema definition	Read	registry*		
			schema*		
GetSchemaVersion	Grants permission to retrieve a schema version	Read	registry		
			schema		
GetSchemaVersionsDiff	Grants permission to compare two schema versions in schema registry	Read	registry*		
			schema*		
GetSecurityConfiguration	Grants permission to retrieve a security configuration	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSecurityConfigurations	Grants permission to retrieve one or more security configurations	Read			
GetSession	Grants permission to retrieve an interactive session	Read	session*		
GetStage	Grants permission to get a stage for SparkUI	Permissions management			
GetStageAttempt	Grants permission to get a stage attempt for SparkUI	Permissions management			
GetStageAttemptTaskList	Grants permission to get the task list for a stage attempt for SparkUI	Permissions management			
GetStageAttemptTaskSummary	Grants permission to get the task summary for a stage attempt for SparkUI	Permissions management			
GetStageFiles	Grants permission to get stage files for SparkUI	Permissions management			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetStages	Grants permission to get stages for SparkUI	Permissions management			
GetStatement	Grants permission to retrieve result and information about a statement in an interactive session	Read	session*		
GetStorage	Grants permission to get storage details for SparkUI	Permissions management			
GetStorageUnit	Grants permission to get storage unit details for SparkUI	Permissions management			
GetTable	Grants permission to retrieve a table	Read	database*		
			rootcatalog*		
			table*		
			catalog		
GetTableOptimizer	Grants permission to return the configuration of all optimizers associated with a specified table	Read	database*		glue:GetTable
			rootcatalog*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			table*		
GetTableVersion	Grants permission to retrieve a version of a table	Read	database*		
			rootcatalog*		
			table*		
			catalog		
GetTableVersions	Grants permission to retrieve a list of versions of a table	Read	database*		
			rootcatalog*		
			table*		
			catalog		
GetTables	Grants permission to retrieve the tables in a database	Read	database*		
			rootcatalog*		
			table*		
			catalog		
GetTags	Grants permission to retrieve all tags associated with a resource	Read	blueprint		
			crawler		
			customEntityType		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			devendpoint		
			job		
			trigger		
			usageProfile		
			workflow		
GetTrigger	Grants permission to retrieve a trigger	Read	trigger*		
GetTriggers	Grants permission to retrieve the triggers associated with a job	Read			
GetUsageProfile	Grants permission to retrieve a usage profile	Read	usageProfile*		
GetUserDefinedFunction	Grants permission to retrieve a function definition	Read	database*		
			rootcatalog*		
			userdefinedfunction*		
			catalog		
	Grants permission to retrieve multiple function definitions	Read	database*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetUserDefinedFunctions			rootcatalog*		
			userdefinedfunction*		
			catalog		
GetWorkflow	Grants permission to retrieve a workflow	Read	workflow*		
GetWorkflowRun	Grants permission to retrieve a workflow run	Read	workflow*		
GetWorkflowRunProperties	Grants permission to retrieve workflow run properties	Read	workflow*		
GetWorkflowRuns	Grants permission to retrieve all runs of a workflow	Read	workflow*		
GlueNotebookAuthorize	Grants permission to access Glue Studio Notebooks	Permissions management			
GlueNotebookRefreshCredentials	Grants permission to refresh Glue Studio Notebooks credentials	Permissions management			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportCatalogToGlue	Grants permission to import an Athena data catalog into Amazon Glue	Write	rootcatalog*		
ListBlueprints	Grants permission to retrieve all blueprints	List			
ListColumnStatisticsTaskRuns	Grants permission to list all Column Statistics run-ids that have been executed for the account	Read			
ListConnectionTypes	Grants permission to list connection types in glue studio	Permissions management			
ListCrawlers	Grants permission to retrieve all crawlers	List			
ListCrawls	Grants permission to retrieve crawl run history for a crawler	List	crawler*		
ListCustomEntityTypes	Grants permission to retrieve all Custom Entity Types	List			
ListDataQualityResults	Grants permission to retrieve all Data Quality results	List	dataQualityRuleset*		
ListDataQualityRuleRecommendationRuns	Grants permission to retrieve all Data Quality rule recommendation runs	List	dataQualityRuleset*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDataQualityRulesetEvaluationRuns	Grants permission to retrieve all Data Quality rule recommendation runs	List	dataQualityRuleset*		
ListDataQualityRulesets	Grants permission to retrieve a list of Data Quality rulesets	List	dataQualityRuleset*		
ListDevEndpoints	Grants permission to retrieve all development endpoints	List			
ListEntities	Grants permission to list entities in glue studio	Permissions management	connection*		
			rootcatalog*		
ListJobUpgradeAnalyses	Grants permission to list upgrade analyses for a job	List	job*		
ListJobs	Grants permission to retrieve all current jobs	List			
ListMLTransforms	Grants permission to retrieve all ML Transforms	List	mlTransform*		
ListRegistries	Grants permission to retrieve a list of schema registries	List			
ListSchemaVersions	Grants permission to retrieve a list of schema versions	List	registry*		
			schema*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListSchemas	Grants permission to retrieve a list of schema containers	List	registry		
ListSessions	Grants permission to retrieve a list of interactive session	List			
ListStatements	Grants permission to retrieve a list of statements in an interactive session	List	session*		
ListTableOptimizerRuns	Grants permission to list the history of previous optimizer runs for a specific table	List	database*		glue:GetTable
			rootcatalog*		
			table*		
ListTriggers	Grants permission to retrieve all triggers	List			
ListUsageProfiles	Grants permission to retrieve a list of usage profiles	List			
ListWorkflows	Grants permission to retrieve all workflows	List			
ModifyIntegration	Grants permission to modify a zero-ETL integration	Write	integration*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
NotifyEvent	Grants permission to notify an event to the event-driven workflow	Write	workflow*		
PassConnection [permission only]	Grants permission to pass glue connection name in input for APIs that require them	Write	connection*		
PublishDataQuality [permission only]	Grants permission to publish Data Quality results	Write	dataQualityRuleset*		
PutDataCatalogEncryptionSettings	Grants permission to update catalog encryption settings	Write	rootcatalog*		
PutDataQualityProfileAnnotation	Grants permission to annotate all datapoints for a profile	Write	dataQualityRuleset*		
			job*		
PutDataQualityStatisticAnnotation	Grants permission to annotate datapoints over time for a specific data quality statistic	Write	dataQualityRuleset*		
			job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutResourcePolicy	Grants permission to update a resource policy	Permissions management	rootcatalog*		
PutSchemaVersionMetadata	Grants permission to add metadata to schema version	Write	registry		
			schema		
PutWorkflowRunProperties	Grants permission to update workflow run properties	Write	workflow*		
QuerySchemaVersionMetadata	Grants permission to fetch metadata for a schema version	List	registry		
			schema		
RefreshOAuth2Tokens	Grants permission to refresh the oauth2 tokens for connection during job execution	Permissions management	connection*		
			rootcatalog*		
RegisterSchemaVersion	Grants permission to create a new schema version	Write	registry*		
			schema*		
RemoveSchemaVersionMetadata	Grants permission to remove metadata from schema version	Write	registry		
			schema		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RequestLogParsing	Grants permission to request log parsing for SparkUI	Permissions management			
ResetJobBookmark	Grants permission to reset a job bookmark	Write			
ResumeWorkflowRun	Grants permission to resume a workflow run	Write	workflow*		
RunDataPreviewStatement	Grants permission to run Data Preview Statement	Permissions management			
RunStatement	Grants permission to run a code or statement in an interactive session	Write	session*		
SearchTables	Grants permission to retrieve the tables in the catalog	Read	database*		
			rootcatalog*		
			table*		
			catalog		
SendFeedback	Grants permission to provide feedback about a glue completion experience in Amazon Q	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendRecipeAction	Grants permission to execute a Data Preparation Recipe statement in data preview	Permissions management			
StartBlueprintRun	Grants permission to start running a blueprint	Write	blueprint*		
StartColumnStatisticsTaskRun	Grants permission to start a run for generating Column Statistics for the table	Write	database*		glue:GetSecurityConfiguration glue:GetTable
			rootcatalog*		
			table*		
StartColumnStatisticsTaskRunSchedule	Grants permission to start a column statistics task run schedule	Write	database*		
			rootcatalog*		
			table*		
StartCompletion	Grants permission to create a completion request in Glue for Amazon Q experience	Write			
StartCrawler	Grants permission to start a crawler	Write	crawler*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartCrawlerSchedule	Grants permission to change the schedule state of a crawler to SCHEDULED	Write			
StartDataQualityRuleRecommendationRun	Grants permission to start a Data Quality rule recommendation run	Write	dataQualityRuleset*		
StartDataQualityRulesetEvaluationRun	Grants permission to start a Data Quality rule recommendation run	Write	dataQualityRuleset*		
StartExportLabelsTaskRun	Grants permission to start an Export Labels ML Task Run	Write	mlTransform*		
StartImportLabelsTaskRun	Grants permission to start an Import Labels ML Task Run	Write	mlTransform*		
StartJobRun	Grants permission to start running a job	Write	job*		
StartJobUpgradeAnalysis	Grants permission to start running upgrade analysis for a job	Write	job*		
StartMLEvaluationTaskRun	Grants permission to start an Evaluation ML Task Run	Write	mlTransform*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartMLLabelingSetGenerationTaskRun	Grants permission to start a Labeling Set Generation ML Task Run	Write	mlTransform*		
StartNotebook	Grants permission to start Glue Studio Notebooks	Permissions management			
StartTrigger	Grants permission to start a trigger	Write	trigger*		
StartWorkflowRun	Grants permission to start running a workflow	Write	workflow*		
StopColumnStatisticsTaskRun	Grants permission to stop execution for Column Statistics run	Write	database*		
			rootcatalog*		
			table*		
StopColumnStatisticsTaskRunSchedule	Grants permission to stop a column statistics task run schedule	Write	database*		
			rootcatalog*		
			table*		
StopCrawler	Grants permission to stop a running crawler	Write	crawler*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopCrawlerSchedule	Grants permission to set the schedule state of a crawler to NOT_SCHEDULED	Write			
StopJobUpgradeAnalysis	Grants permission to stop an on-going upgrade analysis for a job	Write	job*		
StopSession	Grants permission to stop an interactive session	Write	session*		
StopTrigger	Grants permission to stop a trigger	Write	trigger*		
StopWorkflowRun	Grants permission to stop a workflow run	Write	workflow*		
TagResource	Grants permission to add tags to a resource	Tagging	blueprint		
			connection		
			crawler		
			customEntityType		
			dataQualityRuleset		
			devendpoint		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			integration		
			job		
			mlTransform		
			registry		
			schema		
			session		
			trigger		
			usageProfile		
			workflow		
				aws:TagKeys aws:RequestTag/${TagKey}	
Terminate Notebook	Grants permission to terminate Glue Studio Notebooks	Permissions management			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TestConnection	Grants permission to test connection in Glue Studio	Permissions management			
UntagResource	Grants permission to remove tags associated with a resource	Tagging	blueprint		
			connection		
			crawler		
			customEntityType		
			dataQualityRuleset		
			devendpoint		
			integration		
			job		
			mlTransform		
			registry		
			schema		
			session		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			trigger		
			usageProfile		
			workflow		
				aws:TagKeys	
UpdateBlueprint	Grants permission to update a blueprint	Write	blueprint*		
UpdateCatalog	Grants permission to update a catalog	Write	rootcatalog*		
			catalog		
UpdateClassifier	Grants permission to update a classifier	Write			
UpdateColumnStatisticsForPartition	Grants permission to update partition statistics of columns	Write	database*		
			rootcatalog*		
			table*		
			catalog		
UpdateColumnStatisticsForTable	Grants permission to update table statistics of columns	Write	database*		
			rootcatalog*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			table*		
			catalog		
UpdateColumnStatisticsTaskSettings	Grants permission to update settings for a column statistics task	Write	database*		
			rootcatalog*		
			table*		
UpdateConnection	Grants permission to update a connection	Write	connection*		
			rootcatalog*		
UpdateCrawler	Grants permission to update a crawler	Write	crawler*		
UpdateCrawlerSchedule	Grants permission to update the schedule of a crawler	Write			
UpdateDataQualityRuleset	Grants permission to update a Data Quality ruleset	Write	dataQualityRuleset*		
UpdateDatabase	Grants permission to update a database	Write	database*		
			rootcatalog*		
			catalog		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateDevEndpoint	Grants permission to update a development endpoint	Write	devendpoint*		
UpdateIntegrationResourceProperty	Grants permission to update the integration resource property	Write	catalog*		
			connection*		
			database*		
UpdateIntegrationTableProperties	Grants permission to update the integration table properties	Write	catalog*		
			connection*		
			database*		
UpdateJob	Grants permission to update a job	Write	job*		
				glue:VpcIds glue:SubnetIds glue:SecurityGroupIds	
UpdateJobFromSourceControl	Grants permission to update a job from source control provider	Write	job*		
UpdateMLTransform	Grants permission to update an ML Transform	Write	mlTransform*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdatePartition	Grants permission to update a partition	Write	database*		
			rootcatalog*		
			table*		
			catalog		
UpdateRegistry	Grants permission to update a schema registry	Write	registry*		
UpdateSchema	Grants permission to update a schema container	Write	registry*		
			schema*		
UpdateSourceControlFromJob	Grants permission to update source control provider from a job	Write	job*		
UpdateTable	Grants permission to update a table	Write	database*		
			rootcatalog*		
			table*		
			catalog		
UpdateTableOptimizer	Grants permission to update the configuration for an existing table optimizer	Write	database*		glue:GetTable
			rootcatalog*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			table*		
UpdateTrigger	Grants permission to update a trigger	Write	trigger*		
UpdateUsageProfile	Grants permission to update a usage profile	Write	usageProfile*		
UpdateUserDefinedFunction	Grants permission to update a function definition	Write	database*		
			rootcatalog*		
			userdefinedfunction*		
			catalog		
UpdateWorkflow	Grants permission to update a workflow	Write	workflow*		
UpgradeJob	Grants permission to upgrade a job to the latest version	Write	job*		
UseGlueStudio	Grants permission to use Glue Studio and access its internal APIs	Permissions management			
UseMLTransforms [permission only]	Grants permission to use an ML Transform from within a Glue ETL Script	Write	mlTransform*		

Resource types defined by Amazon Glue

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
rootcatalog	`arn:${Partition}:glue:${Region}:${Account}:catalog`	
catalog	`arn:${Partition}:glue:${Region}:${Account}:catalog/${CatalogName}`	
database	`arn:${Partition}:glue:${Region}:${Account}:database/${DatabaseName}`	
table	`arn:${Partition}:glue:${Region}:${Account}:table/${DatabaseName}/${TableName}`	
tableversion	`arn:${Partition}:glue:${Region}:${Account}:tableVersion/${DatabaseName}/${TableName}/${TableVersionName}`	
connection	`arn:${Partition}:glue:${Region}:${Account}:connection/${ConnectionName}`	aws:ResourceTag/${TagKey}
userdefinedfunction	`arn:${Partition}:glue:${Region}:${Account}:userDefinedFunction/${DatabaseName}/${UserDefinedFunctionName}`	
devendpoint	`arn:${Partition}:glue:${Region}:${Account}:devEndpoint/${DevEndpointName}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
job	arn:${Partition}:glue:${Region}:${Account}:job/${JobName}	aws:ResourceTag/${TagKey}
trigger	arn:${Partition}:glue:${Region}:${Account}:trigger/${TriggerName}	aws:ResourceTag/${TagKey}
crawler	arn:${Partition}:glue:${Region}:${Account}:crawler/${CrawlerName}	aws:ResourceTag/${TagKey}
workflow	arn:${Partition}:glue:${Region}:${Account}:workflow/${WorkflowName}	aws:ResourceTag/${TagKey}
blueprint	arn:${Partition}:glue:${Region}:${Account}:blueprint/${BlueprintName}	aws:ResourceTag/${TagKey}
mlTransform	arn:${Partition}:glue:${Region}:${Account}:mlTransform/${TransformId}	aws:ResourceTag/${TagKey}
registry	arn:${Partition}:glue:${Region}:${Account}:registry/${RegistryName}	aws:ResourceTag/${TagKey}
schema	arn:${Partition}:glue:${Region}:${Account}:schema/${SchemaName}	aws:ResourceTag/${TagKey}
session	arn:${Partition}:glue:${Region}:${Account}:session/${SessionId}	aws:ResourceTag/${TagKey}
usageProfile	arn:${Partition}:glue:${Region}:${Account}:usageProfile/${UsageProfileId}	aws:ResourceTag/${TagKey}
dataQualityRuleset	arn:${Partition}:glue:${Region}:${Account}:dataQualityRuleset/${RulesetName}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
customEntityType	`arn:${Partition}:glue:${Region}:${Account}:customEntityType/${CustomEntityTypeId}`	aws:ResourceTag/${TagKey}
completion	`arn:${Partition}:glue:${Region}:${Account}:completion/${CompletionId}`	
integration	`arn:${Partition}:glue:${Region}:${Account}:integration:${IntegrationId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Glue

Amazon Glue 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 Amazon 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
glue:CredentialIssuingService	Filters access by the service from which the credentials of the request is issued	String

Condition keys	Description	Type
glue:EnabledForRedshiftAutoDiscovery	Filters access by the presence of the key configured for role's identity-based policy	Bool
glue:RoleAssumedBy	Filters access by the service from which the credentials of the request is obtained by assuming the customer role	String
glue:SecurityGroupIds	Filters access by the ID of security groups configured for the Glue job	ArrayOfString
glue:SubnetIds	Filters access by the ID of subnets configured for the Glue job	ArrayOfString
glue:VpcIds	Filters access by the ID of the VPC configured for the Glue job	ArrayOfString

Actions, resources, and condition keys for Amazon Glue DataBrew

Amazon Glue DataBrew (service prefix: `databrew`) 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 Glue DataBrew
- Resource types defined by Amazon Glue DataBrew
- Condition keys for Amazon Glue DataBrew

Actions defined by Amazon Glue DataBrew

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 Amazon. 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.

> **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
BatchDeleteRecipeVersion	Grants permission to delete one or more recipe versions	Write	Recipe*		
CreateDataset	Grants permission to create a dataset	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProfileJob	Grants permission to create a profile job	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateProject	Grants permission to create a project	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRecipe	Grants permission to create a recipe	Write		aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
CreateRecipeJob	Grants permission to create a recipe job	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateRuleset	Grants permission to create a ruleset	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateSchedule	Grants permission to create a schedule	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDataset	Grants permission to delete a dataset	Write	Dataset*		
DeleteJob	Grants permission to delete a job	Write	Job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteProject	Grants permission to delete a project	Write	Project*		
DeleteRecipeVersion	Grants permission to delete a recipe version	Write	Recipe*		
DeleteRuleset	Grants permission to delete a ruleset	Write	Ruleset*		
DeleteSchedule	Grants permission to delete a schedule	Write	Schedule*		
DescribeDataset	Grants permission to view details about a dataset	Read	Dataset*		
DescribeJob	Grants permission to view details about a job	Read	Job*		
DescribeJobRun	Grants permission to view details about job run for a given job	Read	Job*		
DescribeProject	Grants permission to view details about a project	Read	Project*		
DescribeRecipe	Grants permission to view details about a recipe	Read	Recipe*		
DescribeRuleset	Grants permission to view details about a ruleset	Read	Ruleset*		
DescribeSchedule	Grants permission to view details about a schedule	Read	Schedule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDatasets	Grants permission to list datasets in your account	Read			
ListJobRuns	Grants permission to list job runs for a given job	Read	Job*		
ListJobs	Grants permission to list jobs in your account	Read			
ListProjects	Grants permission to list projects in your account	Read			
ListRecipeVersions	Grants permission to list versions in your recipe	Read	Recipe*		
ListRecipes	Grants permission to list recipes in your account	Read			
ListRulesets	Grants permission to list rulesets in your account	Read			
ListSchedules	Grants permission to list schedules in your account	Read			
ListTagsForResource	Grants permission to retrieve tags associated with a resource	Read	Dataset		
			Job		
			Project		
			Recipe		
			Ruleset		
			Schedule		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PublishRecipe	Grants permission to publish a major verison of a recipe	Write	Recipe*		
SendProjectSessionAction	Grants permission to submit an action to the interactive session for a project	Write	Project*		
StartJobRun	Grants permission to start running a job	Write	Job*		
StartProjectSession	Grants permission to start an interactive session for a project	Write	Project*		
StopJobRun	Grants permission to stop a job run for a job	Write	Job*		
TagResource	Grants permission to add tags to a resource	Tagging	Dataset		
			Job		
			Project		
			Recipe		
			Ruleset		
			Schedule		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags associated with a resource	Tagging	Dataset		
			Job		
			Project		
			Recipe		
			Ruleset		
			Schedule		
				aws:TagKeys	
UpdateDataset	Grants permission to modify a dataset	Write	Dataset*		
UpdateProfileJob	Grants permission to modify a profile job	Write	Job*		
UpdateProject	Grants permission to modify a project	Write	Project*		
UpdateRecipe	Grants permission to modify a recipe	Write	Recipe*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateRecipeJob	Grants permission to modify a recipe job	Write	Job*		
UpdateRuleset	Grants permission to modify a ruleset	Write	Ruleset*		
UpdateSchedule	Grants permission to modify a schedule	Write	Schedule*		

Resource types defined by Amazon Glue DataBrew

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
Project	`arn:${Partition}:databrew:${Region}:${Account}:project/${ResourceId}`	aws:ResourceTag/${TagKey}
Dataset	`arn:${Partition}:databrew:${Region}:${Account}:dataset/${ResourceId}`	aws:ResourceTag/${TagKey}
Ruleset	`arn:${Partition}:databrew:${Region}:${Account}:ruleset/${ResourceId}`	aws:ResourceTag/${TagKey}
Recipe	`arn:${Partition}:databrew:${Region}:${Account}:recipe/${ResourceId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
Job	`arn:${Partition}:databrew:${Region}:${Account}:job/${ResourceId}`	aws:ResourceTag/${TagKey}
Schedule	`arn:${Partition}:databrew:${Region}:${Account}:schedule/${ResourceId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Glue DataBrew

Amazon Glue DataBrew 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 Amazon 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 GuardDuty

Amazon GuardDuty (service prefix: `guardduty`) 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 GuardDuty
- Resource types defined by Amazon GuardDuty
- Condition keys for Amazon GuardDuty

Actions defined by Amazon GuardDuty

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 Amazon. 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.

> **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 invitations to become a GuardDuty member account	Write			
AcceptInvitation	Grants permission to accept invitations to become a GuardDuty member account	Write			
ArchiveFindings	Grants permission to archive GuardDuty findings	Write			
CreateDetector	Grants permission to create a detector	Write		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateFilter	Grants permission to create GuardDuty filters. A filters defines finding attributes and conditions used to filter findings	Write	filter*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateIPSet	Grants permission to create an IPSet	Write		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	iam:DeleteRolePolicy iam:PutRolePolicy

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateMalwareProtectionPlan	Grants permission to create a new Malware Protection plan	Write		aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
CreateMembers	Grants permission to create GuardDuty member accounts, where the account used to create a member becomes the GuardDuty administrator account	Write			
CreatePublishingDestination	Grants permission to create a publishing destination	Write			s3:GetObject s3:ListBucket
CreateSampleFindings	Grants permission to create sample findings	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateThreatIntelSet	Grants permission to create GuardDuty ThreatIntelSets, where a ThreatIntelSet consists of known malicious IP addresses used by GuardDuty to generate findings	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeclineInvitations	Grants permission to decline invitations to become a GuardDuty member account	Write			
DeleteDetector	Grants permission to delete GuardDuty detectors	Write	detector*		
DeleteFilter	Grants permission to delete GuardDuty filters	Write	filter*		
DeleteIPSet	Grants permission to delete GuardDuty IPSets	Write	ipset*		
DeleteInvitations	Grants permission to delete invitations to become a GuardDuty member account	Write			
DeleteMalwareProtectionPlan	Grants permission to delete a Malware Protection plan	Write	malwareprotectionplan*		
DeleteMembers	Grants permission to delete GuardDuty member accounts	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeletePublishingDestination	Grants permission to delete a publishing destination	Write	publishingDestination*		
DeleteThreatIntelSet	Grants permission to delete GuardDuty ThreatIntelSets	Write	threatintelset*		
DescribeMalwareScans	Grants permission to retrieve details about malware scans	Read			
DescribeOrganizationConfiguration	Grants permission to retrieve details about the delegated administrator associated with a GuardDuty detector	Read			
DescribePublishingDestination	Grants permission to retrieve details about a publishing destination	Read	publishingDestination*		
DisableOrganizationAdminAccount	Grants permission to disable the organization delegated administrator for GuardDuty	Write			
DisassociateFromAdministratorAccount	Grants permission to disassociate a GuardDuty member account from its GuardDuty administrator account	Write			
DisassociateFromMasterAccount	Grants permission to disassociate a GuardDuty member account from its GuardDuty administrator account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateMembers	Grants permission to disassociate GuardDuty member accounts from their administrator GuardDuty account	Write			
EnableOrganizationAdminAccount	Grants permission to enable an organization delegated administrator for GuardDuty	Write			
GetAdministratorAccount	Grants permission to retrieve details of the GuardDuty administrator account associated with a member account	Read			
GetCoverageStatistics	Grants permission to list Amazon GuardDuty coverage statistics for the specified GuardDuty account in a Region	Read	detector*		
GetDetector	Grants permission to retrieve GuardDuty detectors	Read	detector*		
GetFilter	Grants permission to retrieve GuardDuty filters	Read	filter*		
GetFindings	Grants permission to retrieve GuardDuty findings	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetFindingsStatistics	Grants permission to retrieve a list of GuardDuty finding statistics	Read			
GetIPSet	Grants permission to retrieve GuardDuty IPSets	Read	ipset*		
GetInvitationsCount	Grants permission to retrieve the count of all GuardDuty invitations sent to a specified account, which does not include the accepted invitation	Read			
GetMalwareProtectionPlan	Grants permission to retrieve a Malware Protection plan details	Read	malwareprotectionplan*		
GetMalwareScanSettings	Grants permission to retrieve the malware scan settings	Read			
GetMasterAccount	Grants permission to retrieve details of the GuardDuty administrator account associated with a member account	Read			
GetMemberDetectors	Grants permission to describe which data sources are enabled for member accounts detectors	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetMembers	Grants permission to retrieve the member accounts associated with an administrator account	Read			
GetOrganizationStatistics	Grants permission to retrieve GuardDuty protection plan coverage statistics for member accounts in a Region	Read			
GetRemainingFreeTrialDays	Grants permission to provide the number of days left for each data source used in the free trial period	Read			
GetThreatIntelSet	Grants permission to retrieve GuardDuty ThreatIntelSets	Read	threatintelset*		
GetUsageStatistics	Grants permission to list Amazon GuardDuty usage statistics over the last 30 days for the specified detector ID	Read			
InviteMembers	Grants permission to invite other Amazon accounts to enable GuardDuty and become GuardDuty member accounts	Write			
ListCoverage	Grants permission to list all the resource details for a given account in a Region	List	detector*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDetectors	Grants permission to retrieve a list of GuardDuty detectors	List			
ListFilters	Grants permission to retrieve a list of GuardDuty filters	List			
ListFindings	Grants permission to retrieve a list of GuardDuty findings	List			
ListIPSets	Grants permission to retrieve a list of GuardDuty IPSets	List			
ListInvitations	Grants permission to retrieve a list of all of the GuardDuty membership invitations that were sent to an Amazon Web Services account	List			
ListMalwareProtectionPlans	Grants permission to retrieve a list of Malware Protection plans	List			
ListMembers	Grants permission to retrieve a list of GuardDuty member accounts associated with an administrator account	List			
ListOrganizationAdminAccounts	Grants permission to list details about the organization delegated administrator for GuardDuty	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPublishingDestinations	Grants permission to retrieve a list of publishing destinations	List			
ListTagsForResource	Grants permission to retrieve a list of tags associated with a GuardDuty resource	Read	detector		
			filter		
			ipset		
			malwareprotectionplan		
			threatintelset		
ListThreatIntelSets	Grants permission to retrieve a list of GuardDuty ThreatIntelSets	List			
SendSecurityTelemetry	Grants permission to send security telemetry for a specific GuardDuty account in a Region	Write			
StartMalwareScan	Grants permission to initiate a new malware scan	Write			
StartMonitoringMembers	Grants permission to a GuardDuty administrator account to monitor findings from GuardDuty member accounts	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopMonitoringMembers	Grants permission to disable monitoring findings from member accounts	Write			
TagResource	Grants permission to add tags to a GuardDuty resource	Tagging	detector		
			filter		
			ipset		
			malwareprotectionplan		
			threatintelset		
				aws:RequestTag/${TagKey} aws:TagKeys	
UnarchiveFindings	Grants permission to unarchive GuardDuty findings	Write			
UntagResource	Grants permission to remove tags from a GuardDuty resource	Tagging	detector		
			filter		
			ipset		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			malwareprotectionplan		
			threatintelset		
				aws:TagKeys	
UpdateDetector	Grants permission to update GuardDuty detectors	Write	detector*		
UpdateFilter	Grants permission to updates GuardDuty filters	Write	filter*		
UpdateFindingsFeedback	Grants permission to update findings feedback to mark GuardDuty findings as useful or not useful	Write			
UpdateIPSet	Grants permission to update GuardDuty IPSets	Write	ipset*		iam:DeleteRolePolicy iam:PutRolePolicy
UpdateMalwareProtectionPlan	Grants permission to update the Malware Protection plan	Write	malwareprotectionplan*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateMalwareScanSettings	Grants permission to update the malware scan settings	Write			
UpdateMemberDetectors	Grants permission to update which data sources are enabled for member accounts detectors	Write			
UpdateOrganizationConfiguration	Grants permission to update the delegated administrator configuration associated with a GuardDuty detector	Write			
UpdatePublishingDestination	Grants permission to update a publishing destination	Write	publishingDestination*		s3:GetObject s3:ListBucket
UpdateThreatIntelSet	Grants permission to updates the GuardDuty ThreatIntelSets	Write	threatintelset*		iam:DeleteRolePolicy iam:PutRolePolicy

Resource types defined by Amazon GuardDuty

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
detector	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}`	aws:ResourceTag/${TagKey}
filter	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/filter/${FilterName}`	aws:ResourceTag/${TagKey}
ipset	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/ipset/${IPSetId}`	aws:ResourceTag/${TagKey}
threatintelset	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/threatintelset/${ThreatIntelSetId}`	aws:ResourceTag/${TagKey}
publishingDestination	`arn:${Partition}:guardduty:${Region}:${Account}:detector/${DetectorId}/publishingDestination/${PublishingDestinationId}`	
malwareprotectionplan	`arn:${Partition}:guardduty:${Region}:${Account}:malware-protection-plan/${MalwareProtectionPlanId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon GuardDuty

Amazon GuardDuty 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 Amazon global condition context keys.

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

Actions, resources, and condition keys for Amazon Health APIs and Notifications

Amazon 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 Amazon Health APIs and Notifications
- Resource types defined by Amazon Health APIs and Notifications
- Condition keys for Amazon Health APIs and Notifications

Actions defined by Amazon 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 Amazon. 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.

> **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*		
				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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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
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 Amazon 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 Amazon Health APIs and Notifications

Amazon 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 Amazon 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 Amazon IAM Access Analyzer

Amazon IAM Access Analyzer (service prefix: `access-analyzer`) 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 IAM Access Analyzer
- Resource types defined by Amazon IAM Access Analyzer
- Condition keys for Amazon IAM Access Analyzer

Actions defined by Amazon IAM Access Analyzer

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 Amazon. 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.

> **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
ApplyArchiveRule	Grants permission to apply an archive rule	Write	Analyzer*		
CancelPolicyGeneration	Grants permission to cancel a policy generation	Write			
CheckAccessNotGranted	Grants permission to check that specified access is not allowed by a policy	Read			
CheckNoNewAccess	Grants permission to check that no new access is allowed when compared to an existing policy	Read			
CheckNoPublicAccess	Grants permission to check that public access is not allowed by a resource policy	Read			
CreateAccessPreview	Grants permission to create an access preview for the specified analyzer	Write	Analyzer*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAnalyzer	Grants permission to create an analyzer	Write	Analyzer*		iam:CreateServiceLinkedRole
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateArchiveRule	Grants permission to create an archive rule for the specified analyzer	Write	ArchiveRule*		
DeleteAnalyzer	Grants permission to delete the specified analyzer	Write	Analyzer*		
DeleteArchiveRule	Grants permission to delete archive rules for the specified analyzer	Write	ArchiveRule*		
GenerateFindingRecommendation	Grants permission to generate recommendation steps to resolve a finding	Write	Analyzer*		
GetAccessPreview	Grants permission to retrieve information about an access preview	Read	Analyzer*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAnalyzedResource	Grants permission to retrieve information about an analyzed resource	Read	Analyzer*		
GetAnalyzer	Grants permission to retrieve information about analyzers	Read	Analyzer*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GetArchiveRule	Grants permission to retrieve information about archive rules for the specified analyzer	Read	ArchiveRule*		
GetFinding	Grants permission to retrieve findings	Read	Analyzer*		
GetFindingRecommendation	Grants permission to retrieve recommendation steps to resolve a finding	Read	Analyzer*		
GetFindingsStatistics	Grants permission to retrieve statistics for findings	Read	Analyzer*		
GetGeneratedPolicy	Grants permission to retrieve a policy that was generated using StartPolicyGeneration	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAccessPreviewFindings	Grants permission to retrieve a list of findings from an access preview	Read	Analyzer*		
ListAccessPreviews	Grants permission to retrieve a list of access previews	List	Analyzer*		
ListAnalyzedResources	Grants permission to retrieve a list of resources that have been analyzed	Read	Analyzer*		
ListAnalyzers	Grants permission to retrieves a list of analyzers	List			
ListArchiveRules	Grants permission to retrieve a list of archive rules from an analyzer	List	Analyzer*		
ListFindings	Grants permission to retrieve a list of findings from an analyzer	Read	Analyzer*		
ListPolicyGenerations	Grants permission to list all the recently started policy generations	Read			
ListTagsForResource	Grants permission to retrieve a list of tags applied to a resource	Read	Analyzer		
StartPolicyGeneration	Grants permission to start a policy generation	Write			iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartResourceScan	Grants permission to start a scan of the policies applied to a resource	Write	Analyzer*		
TagResource	Grants permission to add a tag to a resource	Tagging	Analyzer		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove a tag from a resource	Tagging	Analyzer		
				aws:TagKeys	
UpdateAnalyzer	Grants permission to modify an analyzer's configuration	Write	Analyzer*		
UpdateArchiveRule	Grants permission to modify an archive rule	Write	ArchiveRule*		
UpdateFindings	Grants permission to modify findings	Write	Analyzer*		
ValidatePolicy	Grants permission to validate a policy	Read			

Resource types defined by Amazon IAM Access Analyzer

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
Analyzer	`arn:${Partition}:access-analyzer:${Region}:${Account}:analyzer/${AnalyzerName}`	aws:ResourceTag/${TagKey}
ArchiveRule	`arn:${Partition}:access-analyzer:${Region}:${Account}:analyzer/${AnalyzerName}/archive-rule/${RuleName}`	

Condition keys for Amazon IAM Access Analyzer

Amazon IAM Access Analyzer 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 Amazon global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters actions based on the presence of tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters actions based on tag key-value pairs attached to the resource	String

Condition keys	Description	Type
aws:TagKeys	Filters actions based on the presence of tag keys in the request	ArrayOfString

Actions, resources, and condition keys for Amazon IAM Identity Center (successor to Amazon Single Sign-On)

Amazon IAM Identity Center (successor to Amazon Single Sign-On) (service prefix: `sso`) 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 IAM Identity Center (successor to Amazon Single Sign-On)
- Resource types defined by Amazon IAM Identity Center (successor to Amazon Single Sign-On)
- Condition keys for Amazon IAM Identity Center (successor to Amazon Single Sign-On)

Actions defined by Amazon IAM Identity Center (successor to Amazon Single Sign-On)

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 Amazon. 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.

> **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 Directory	Grants permission to connect a directory to be used by Amazon IAM Identity Center	Write			ds:AuthorizeApplication

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateProfile	Grants permission to create an association between a directory user or group and a profile	Write			
AttachCustomerManagedPolicyReferenceToPermissionSet	Grants permission to attach a customer managed policy reference to a permission set	Permissions management	Instance*		
			PermissionSet*		
AttachManagedPolicyToPermissionSet	Grants permission to attach an Amazon managed policy to a permission set	Permissions management	Instance*		
			PermissionSet*		
CreateAccountAssignment	Grants permission to assign access to a Principal for a specified Amazon Web Services account using a specified permission set	Write	Account*		
			Instance*		
			PermissionSet*		
CreateApplication	Grants permission to create an application	Write	ApplicationProvider*		
			Instance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateApplicationAssignment	Grants permission to create an application assignment	Write	Application*		
				sso:ApplicationAccount	
CreateApplicationInstance	Grants permission to add an application instance to Amazon IAM Identity Center	Write			
CreateApplicationInstanceCertificate	Grants permission to add a new certificate for an application instance	Write			
CreateInstance	Grants permission to create an identity center instance	Write	Instance*		iam:CreateServiceLinkedRole organizations:DescribeOrganization

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
CreateInstanceAccessControlAttributeConfiguration	Grants permission to enable the instance for ABAC and specify the attributes	Write	Instance*		iam:AttachRolePolicy iam:CreateRole iam:DeleteRole iam:DeleteRolePolicy iam:DetachRolePolicy iam:GetRole iam:ListAttachedRolePolicies iam:ListRolePolicies iam:PutRolePolicy

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					iam:UpdateAssumeRolePolicy
CreateManagedApplicationInstance	Grants permission to add a managed application instance to Amazon IAM Identity Center	Write			
CreatePermissionSet	Grants permission to create a permission set	Write	Instance*		
			PermissionSet*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProfile	Grants permission to create a profile for an application instance	Write			
CreateTrust	Grants permission to create a federation trust in a target account	Write			
CreateTrustedTokenIssuer	Grants permission to create a trusted token issuer for an instance	Write	Instance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccountAssignment	Grants permission to delete a Principal's access from a specified Amazon Web Services account using a specified permission set	Write	Account*		
			Instance*		
			PermissionSet*		
DeleteApplication	Grants permission to delete an application	Write	Application*		
				sso:ApplicationAccount	
DeleteApplicationAccessScope	Grants permission to delete an access scope to an application	Write	Application*		
				sso:ApplicationAccount	
DeleteApplicationAssignment	Grants permission to delete an application assignment	Write	Application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sso:ApplicationAccount	
DeleteApplicationAuthenticationMethod	Grants permission to delete an authentication method to an application	Write	Application*		
				sso:ApplicationAccount	
DeleteApplicationGrant	Grants permission to delete a grant from an application	Write	Application*		
				sso:ApplicationAccount	
DeleteApplicationInstance	Grants permission to delete the application instance	Write			
DeleteApplicationInstanceCertificate	Grants permission to delete an inactive or expired certificate from the application instance	Write			
DeleteInlinePolicyFromPermissionSet	Grants permission to delete the inline policy from a specified permission set	Write	Instance*		
			PermissionSet*		
DeleteInstance	Grants permission to delete an identity center instance	Write	Instance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteInstanceAccessControlAttributeConfiguration	Grants permission to disable ABAC and remove the attributes list for the instance	Write	Instance*		
DeleteManagedApplicationInstance	Grants permission to delete the managed application instance	Write			
DeletePermissionSet	Grants permission to delete a permission set	Write	Instance*		
			PermissionSet*		
DeletePermissionsBoundaryFromPermissionSet	Grants permission to remove permissions boundary from a permission set	Permissions management	Instance*		
			PermissionSet*		
DeletePermissionsPolicy	Grants permission to delete the permission policy associated with a permission set	Permissions management			
DeleteProfile	Grants permission to delete the profile for an application instance	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTrustedTokenIssuer	Grants permission to delete a trusted token issuer for an instance	Write	TrustedTokenIssuer*		
DescribeAccountAssignmentCreationStatus	Grants permission to describe the status of the assignment creation request	Read	Instance*		
DescribeAccountAssignmentDeletionStatus	Grants permission to describe the status of an assignment deletion request	Read	Instance*		
DescribeApplication	Grants permission to obtain information about an application	Read	Application*		
				sso:ApplicationAccount	
DescribeApplicationAssignment	Grants permission to retrieve an application assignment	Read	Application*		
				sso:ApplicationAccount	
DescribeApplicationProvider	Grants permission to describe an application provider	Read	ApplicationProvider*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDirectories	Grants permission to obtain information about the directories for this account	Read			
DescribeInstance	Grants permission to obtain information about an identity center instance	Read	Instance*		
DescribeInstanceAccessControlAttributeConfiguration	Grants permission to get the list of attributes used by the instance for ABAC	Read	Instance*		
DescribePermissionSet	Grants permission to describe a permission set	Read	Instance*		
			PermissionSet*		
DescribePermissionSetProvisioningStatus	Grants permission to describe the status for the given Permission Set Provisioning request	Read	Instance*		
DescribePermissionsPolicies	Grants permission to retrieve all the permissions policies associated with a permission set	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeRegisteredRegions	Grants permission to obtain the regions where your organization has enabled Amazon IAM Identity Center	Read			
DescribeTrustedTokenIssuer	Grants permission to describe a trusted token issuer for an instance	Read	TrustedTokenIssuer*		
DescribeTrusts	Grants permission to obtain information about the trust relationships for this account	Read			
DetachCustomerManagedPolicyReferenceFromPermissionSet	Grants permission to detach a customer managed policy reference from a permission set	Permissions management	Instance* PermissionSet*		
DetachManagedPolicyFromPermissionSet	Grants permission to detach the attached Amazon managed policy from the specified permission set	Permissions management	Instance* PermissionSet*		
DisassociateDirectory	Grants permission to disassociate a directory to be used by Amazon IAM Identity Center	Write			ds:UnauthorizeApplication
DisassociateProfile	Grants permission to disassociate a directory user or group from a profile	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetApplicationAccessScope	Grants permission to get an access scope to an application	Read	Application*		
				sso:ApplicationAccount	
GetApplicationAssignmentConfiguration	Grants permission to read assignment configurations for an application	Read	Application*		
				sso:ApplicationAccount	
GetApplicationAuthenticationMethod	Grants permission to get an authentication method to an application	Read	Application*		
				sso:ApplicationAccount	
GetApplicationGrant	Grants permission to obtain details about a grant belonging to an application	Read	Application*		
				sso:ApplicationAccount	
GetApplicationInstance	Grants permission to retrieve details for an application instance	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetApplicationTemplate	Grants permission to retrieve application template details	Read			
GetInlinePolicyForPermissionSet	Grants permission to obtain the inline policy assigned to the permission set	Read	Instance*		
			PermissionSet*		
GetManagedApplicationInstance	Grants permission to retrieve details for an application instance	Read			
GetMfaDeviceManagementForDirectory	Grants permission to retrieve Mfa Device Management settings for the directory	Read			
GetPermissionSet	Grants permission to retrieve details of a permission set	Read			
GetPermissionsBoundaryForPermissionSet	Grants permission to get permissions boundary for a permission set	Read	Instance*		
			PermissionSet*		
GetPermissionsPolicy	Grants permission to retrieve all permission policies associated with a permission set	Read			sso:DescribePermissionsPolicies

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetProfile	Grants permission to retrieve a profile for an application instance	Read			
GetSSOStatus	Grants permission to check if Amazon IAM Identity Center is enabled	Read			
GetSharedSsoConfiguration	Grants permission to retrieve shared configuration for the current SSO instance	Read			
GetSsoConfiguration	Grants permission to retrieve configuration for the current SSO instance	Read			
GetTrust	Grants permission to retrieve the federation trust in a target account	Read			
ImportApplicationInstanceServiceProviderMetadata	Grants permission to update the application instance by uploading an application SAML metadata file provided by the service provider	Write			
ListAccountAssignmentCreationStatus	Grants permission to list the status of the Amazon Web Services account assignment creation requests for a specified SSO instance	List	Instance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAccountAssignmentDeletionStatus	Grants permission to list the status of the Amazon Web Services account assignment deletion requests for a specified SSO instance	List	Instance*		
ListAccountAssignments	Grants permission to list the assignee of the specified Amazon Web Services account with the specified permission set	List	Account*		
			Instance*		
			PermissionSet*		
ListAccountAssignmentsForPrincipal	Grants permission to list accounts assigned to user or group	List	Instance*		
ListAccountsForProvisionedPermissionSet	Grants permission to list all the Amazon accounts where the specified permission set is provisioned	List	Instance*		
			PermissionSet*		
ListApplicationAccessScopes	Grants permission to list access scopes to an application	List	Application*		
				sso:ApplicationAccount	
ListApplicationAssignments	Grants permission to list application assignments	List	Application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sso:ApplicationAccount	
ListApplicationAssignmentsForPrincipal	Grants permission to list applications assigned to user or group	List	Instance*		
				sso:ApplicationAccount	
ListApplicationAuthenticationMethods	Grants permission to list authentication methods to an application	List	Application*		
				sso:ApplicationAccount	
ListApplicationGrants	Grants permission to list grants from an application	List	Application*		
				sso:ApplicationAccount	
ListApplicationInstanceCertificates	Grants permission to retrieve all of the certificates for a given application instance	Read			
ListApplicationInstances	Grants permission to retrieve all application instances	List			sso:GetApplicationInstance

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListApplicationProviders	Grants permission to list application providers	List	ApplicationProvider*		
ListApplicationTemplates	Grants permission to retrieve all supported application templates	List			sso:GetApplicationTemplate
ListApplications	Grants permission to retrieve all applications associated with the instance of IAM Identity Center	List			
ListCustomerManagedPolicyReferencesInPermissionSet	Grants permission to list the customer managed policy references that are attached to a permission set	List	Instance*		
			PermissionSet*		
ListDirectoryAssociations	Grants permission to retrieve details about the directory connected to Amazon IAM Identity Center	Read			
ListInstances	Grants permission to list the SSO Instances that the caller has access to	List			
ListManagedPoliciesInPermissionSet	Grants permission to list the Amazon managed policies that are attached to a specified permission set	List	Instance*		
			PermissionSet*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPermissionSetProvisioningStatus	Grants permission to list the status of the Permission Set Provisioning requests for a specified SSO instance	List	Instance*		
ListPermissionSets	Grants permission to retrieve all permission sets	List	Instance*		
ListPermissionSetsProvisionedToAccount	Grants permission to list all the permission sets that are provisioned to a specified Amazon Web Services account	List	Account*		
			Instance*		
ListProfileAssociations	Grants permission to retrieve the directory user or group associated with the profile	Read			
ListProfiles	Grants permission to retrieve all profiles for an application instance	List			sso:GetProfile
ListTagsForResource	Grants permission to list the tags that are attached to a specified resource	Read	Application		
			Instance		
			PermissionSet		
			TrustedTokenIssuer		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTrustedTokenIssuers	Grants permission to list trusted token issuers for an instance	List	Instance*		
ProvisionPermissionSet	Grants permission to provision a specified permission set to the specified target	Write	Account*		
			Instance*		
			PermissionSet*		
PutApplicationAccessScope	Grants permission to create/update an access scope to an application	Write	Application*		
				sso:ApplicationAccount	
PutApplicationAssignmentConfiguration	Grants permission to add assignment configurations to an application	Write	Application*		
				sso:ApplicationAccount	
PutApplicationAuthenticationMethod	Grants permission to create/update an authentication method to an application	Write	Application*		
				sso:ApplicationAccount	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutApplicationGrant	Grants permission to create/update a grant to an application	Write	Application*		
				sso:ApplicationAccount	
PutInlinePolicyToPermissionSet	Grants permission to attach an IAM inline policy to a permission set	Write	Instance*		
			PermissionSet*		
PutMfaDeviceManagementForDirectory	Grants permission to put Mfa Device Management settings for the directory	Write			
PutPermissionsBoundaryToPermissionSet	Grants permission to add permissions boundary to a permission set	Permissions management	Instance*		
			PermissionSet*		
PutPermissionsPolicy	Grants permission to add a policy to a permission set	Permissions management			
SearchGroups	Grants permission to search for groups within the associated directory	Read			ds:DescribeDirectories
SearchUsers	Grants permission to search for users within the associated directory	Read			ds:DescribeDirectories

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartSSO	Grants permission to initialize Amazon IAM Identity Center	Write			organizations:DescribeOrganization organizations:EnableAWSServiceAccess
TagResource	Grants permission to associate a set of tags with a specified resource	Tagging	Application		
			Instance		
			PermissionSet		
			TrustedTokenIssuer		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to disassociate a set of tags from a specified resource	Tagging	Application		
			Instance		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			PermissionSet		
			TrustedTokenIssuer		
				aws:TagKeys	
UpdateApplication	Grants permission to update an application	Write	Application*		
				sso:ApplicationAccount	
UpdateApplicationInstanceActiveCertificate	Grants permission to set a certificate as the active one for this application instance	Write			
UpdateApplicationInstanceDisplayData	Grants permission to update display data of an application instance	Write			
UpdateApplicationInstanceResponseConfiguration	Grants permission to update federation response configuration for the application instance	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateApplicationInstanceResponseSchemaConfiguration	Grants permission to update federation response schema configuration for the application instance	Write			
UpdateApplicationInstanceSecurityConfiguration	Grants permission to update security details for the application instance	Write			
UpdateApplicationInstanceServiceProviderConfiguration	Grants permission to update service provider related configuration for the application instance	Write			
UpdateApplicationInstanceStatus	Grants permission to update the status of an application instance	Write			
UpdateDirectoryAssociation	Grants permission to update the user attribute mappings for your connected directory	Write			
UpdateInstance	Grants permission to update an identity center instance	Write	Instance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateInstanceAccessControlAttributeConfiguration	Grants permission to update the attributes to use with the instance for ABAC	Write	Instance*		
UpdateManagedApplicationInstanceStatus	Grants permission to update the status of a managed application instance	Write			
UpdatePermissionSet	Grants permission to update the permission set	Permissions management	Instance*		
			PermissionSet*		
UpdateProfile	Grants permission to update the profile for an application instance	Write			
UpdateSSOConfiguration	Grants permission to update the configuration for the current SSO instance	Write			
UpdateTrust	Grants permission to update the federation trust in a target account	Write			
UpdateTrustedTokenIssuer	Grants permission to update a trusted token issuer for an instance	Write	TrustedTokenIssuer*		

Resource types defined by Amazon IAM Identity Center (successor to Amazon Single Sign-On)

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
PermissionSet	`arn:${Partition}:sso:::permissionSet/${InstanceId}/${PermissionSetId}`	aws:ResourceTag/${TagKey}
Account	`arn:${Partition}:sso:::account/${AccountId}`	
Instance	`arn:${Partition}:sso:::instance/${InstanceId}`	aws:ResourceTag/${TagKey}
Application	`arn:${Partition}:sso::${AccountId}:application/${InstanceId}/${ApplicationId}`	aws:ResourceTag/${TagKey} sso:ApplicationAccount
TrustedTokenIssuer	`arn:${Partition}:sso::${AccountId}:trustedTokenIssuer/${InstanceId}/${TrustedTokenIssuerId}`	aws:ResourceTag/${TagKey}
ApplicationProvider	`arn:${Partition}:sso::aws:applicationProvider/${ApplicationProviderId}`	

Condition keys for Amazon IAM Identity Center (successor to Amazon Single Sign-On)

Amazon IAM Identity Center (successor to Amazon Single Sign-On) 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 Amazon 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
sso:ApplicationAccount	Filters access by the account which creates the application. This condition key is not supported for customer managed SAML applications	String

Actions, resources, and condition keys for Amazon IAM Identity Center (successor to Amazon Single Sign-On) directory

Amazon IAM Identity Center (successor to Amazon Single Sign-On) 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 Amazon IAM Identity Center (successor to Amazon Single Sign-On) directory
- Resource types defined by Amazon IAM Identity Center (successor to Amazon Single Sign-On) directory
- Condition keys for Amazon IAM Identity Center (successor to Amazon Single Sign-On) directory

Actions defined by Amazon IAM Identity Center (successor to Amazon Single Sign-On) 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 Amazon. 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.

> **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 Amazon IAM Identity Center provides by default	Write			
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 Amazon 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			
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 Amazon IAM Identity Center provides by default	Write			
CreateProvisioningTenant	Grants permission to create a provisioning tenant for a given directory	Write			
CreateUser	Grants permission to create a user in the directory that Amazon IAM Identity Center provides by default	Write			
DeleteBearerToken	Grants permission to delete a bearer token	Write			
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 Amazon IAM Identity Center provides by default	Write			
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			
DeleteUser	Grants permission to delete a user from the directory that Amazon IAM Identity Center provides by default	Write			
DescribeDirectory	Grants permission to retrieve information about the directory that Amazon IAM Identity Center provides by default	Read			
DescribeGroup	Grants permission to query the group data, not including user and group members	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeGroups	Grants permission to retrieve information about groups from the directory that Amazon IAM Identity Center provides by default	Read			
DescribeProvisioningTenant	Grants permission to describes the provisioning tenant	Read			
DescribeUser	Grants permission to retrieve information about a user from the directory that Amazon IAM Identity Center provides by default	Read			
DescribeUserByUniqueAttribute	Grants permission to describe user with a valid unique attribute represented for the user	Read			
DescribeUsers	Grants permission to retrieve information about user from the directory that Amazon IAM Identity Center provides by default	Read			
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 Amazon IAM Identity Center provides by default	Write			
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 Amazon IAM Identity Center provides by default	Write			
GetAWSSPConfigurationForDirectory	Grants permission to retrieve the Amazon IAM Identity Center Service Provider configurations for the directory	Read			
GetGroupId	Grants permission to retrieve ID information about group from the directory that Amazon IAM Identity Center provides by default	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetUserId	Grants permission to retrieve ID information about user from the directory that Amazon IAM Identity Center provides by default	Read			
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 Amazon IAM Identity Center provides by default	Read			
IsMemberInGroups	Grants permission to check if a member is a part of multiple groups in the directory that Amazon IAM Identity Center provides by default	Read			
ListBearerTokens	Grants permission to list bearer tokens for a given provisioning tenant	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListExternalIdPCertificates	Grants permission to list the external IdP certificates of a given directory and IdP	Read			
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 Amazon IAM Identity Center provides by default	Read			
ListGroupsForMember	Grants permission to list groups of the target member	Read			
ListGroupsForUser	Grants permission to list groups for a user from the directory that Amazon IAM Identity Center provides by default	Read			
ListMembersInGroup	Grants permission to retrieve all members that are part of a group in the directory that Amazon IAM Identity Center provides by default	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListMfaDevicesForUser	Grants permission to list all active MFA devices and their MFA device metadata for a user	Read			
ListProvisioningTenants	Grants permission to list provisioning tenants for a given directory	Read			
ListUsers	Grants permission to list users from the directory that Amazon IAM Identity Center provides by default	Read			
RemoveMemberFromGroup	Grants permission to remove a member that is part of a group in the directory that Amazon IAM Identity Center provides by default	Write			
SearchGroups	Grants permission to search for groups within the associated directory	Read			
SearchUsers	Grants permission to search for users within the associated directory	Read			
StartVirtualMfaDeviceRegistration	Grants permission to begin the creation process of virtual mfa device	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartWebAuthnDeviceRegistration	Grants permission to begin the registration process of a WebAuthn device	Write			
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 Amazon IAM Identity Center provides by default	Write			
UpdateGroupDisplayName	Grants permission to update group display name update group display name response	Write			
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 Amazon IAM Identity Center provides by default	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateUser	Grants permission to update user information in the directory that Amazon IAM Identity Center provides by default	Write			
UpdateUserName	Grants permission to update user name update user name response	Write			
VerifyEmail	Grants permission to verify an email address of an User	Write			

Resource types defined by Amazon IAM Identity Center (successor to Amazon Single Sign-On) directory

Amazon IAM Identity Center (successor to Amazon Single Sign-On) directory does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon IAM Identity Center (successor to Amazon Single Sign-On) directory, specify `"Resource": "*"` in your policy.

Condition keys for Amazon IAM Identity Center (successor to Amazon Single Sign-On) directory

IAM Identity Center (successor to Amazon SSO) 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 Amazon global condition context keys.

Actions, resources, and condition keys for Amazon IAM Identity Center OIDC service

Amazon IAM Identity Center OIDC service (service prefix: `sso-oauth`) 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 IAM Identity Center OIDC service
- Resource types defined by Amazon IAM Identity Center OIDC service
- Condition keys for Amazon IAM Identity Center OIDC service

Actions defined by Amazon IAM Identity Center OIDC 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 Amazon. 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.

> **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
CreateTokenWithIAM	Grants permission to create OAuth/OIDC tokens to access IAM Identity Center integrated applications	Write	Application*		

Resource types defined by Amazon IAM Identity Center OIDC 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
Application	`arn:${Partition}:sso::${AccountId}:application/${InstanceId}/${ApplicationId}`	

Condition keys for Amazon IAM Identity Center OIDC service

OIDC service 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 Amazon global condition context keys.

Actions, resources, and condition keys for Amazon Identity and Access Management (IAM)

Amazon 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 Amazon Identity and Access Management (IAM)
- Resource types defined by Amazon Identity and Access Management (IAM)
- Condition keys for Amazon Identity and Access Management (IAM)

Actions defined by Amazon 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 Amazon. 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.

> **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
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
AddUserToGroup	Grants permission to add an IAM user to the specified IAM group	Write	group*		
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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				iam:PermissionsBoundary	
ChangePassword	Grants permission to an IAM user to change their own password	Write	user*		
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 Amazon Web Services account	Write			
CreateGroup	Grants permission to create a new group	Write	group*		
CreateInstanceProfile	Grants permission to create a new instance profile	Write	instance-profile*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateLoginProfile	Grants permission to create a password for the specified IAM user	Write	user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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}	
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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 Amazon service to perform actions on your behalf	Write	role*		
				iam:AWSServiceName	
CreateServiceSpecificCredential	Grants permission to create a new service-specific credential for an IAM user	Write	user*		
CreateUser	Grants permission to create a new IAM user	Write	user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				iam:PermissionsBoundary aws:TagKeys aws:RequestTag/${TagKey}	
CreateVirtualMFADevice	Grants permission to create a new virtual MFA device	Write	mfa*		
				aws:TagKeys aws:RequestTag/${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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteAccountAlias	Grants permission to delete the specified Amazon Web Services account alias	Write			
DeleteAccountPasswordPolicy	Grants permission to delete the password policy for the Amazon Web Services account	Permissions management			
DeleteCloudFrontPublicKey	Grants permission to delete an existing CloudFront public key	Write			
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*		

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 Amazon 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*		
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	
	Grants permission to delete a virtual MFA device	Write	mfa		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVirtualMFADevice			sms-mfa		
DetachGroupPolicy	Grants permission to detach a managed policy from the specified IAM group	Permissions management	group*		
				iam:PolicyARN	
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableOrganizationsRootSessions	Grants permission to disable privileged root actions in member accounts for an organization managed under the current account	Write			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableOrganizationsRootSessions	Grants permission to enable privileged root actions in member accounts for an organization managed under the current account	Write			
GenerateCredentialReport	Grants permission to generate a credential report for the Amazon Web Services account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GenerateOrganizationsAccessReport	Grants permission to generate an access report for an Amazon 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 Amazon Web Services 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 Amazon Web Services 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 Amazon Web Services 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 Amazon Web Services account	Read			
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*		
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*		
GetOrganizationsAccessReport	Grants permission to retrieve an Amazon Organizations access report	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
GetRolePolicy	Grants permission to retrieve an inline policy document that is embedded with the specified IAM role	Read	role*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
GetUser	Grants permission to retrieve information about the specified IAM user, including the user's creation date, path, unique ID, and ARN	Read	user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 Amazon Web Services 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*		
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			

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 Amazon Web Services account	List			
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*		

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ResyncMFADevice	Grants permission to synchronize the specified MFA device with its IAM entity (user or role)	Write	user*		
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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagInstanceProfile	Grants permission to add tags to an instance profile	Tagging	instance-profile*		
				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 Amazon Web Services account	Write			
UpdateAssumeRolePolicy	Grants permission to update the policy that grants an IAM entity permission to assume a role	Permissions management	role*		
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*		
UpdateRoleDescription	Grants permission to update only the description of a role	Write	role*		
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*		
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 Amazon Web Services account	Write	server-certificate*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UploadSigningCertificate	Grants permission to upload an X.509 signing certificate and associate it with the specified IAM user	Write	user*		

Resource types defined by Amazon 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}/${RoleSessionName}`	
federated-user	`arn:${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}

Resource types	ARN	Condition keys
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}	
user	arn:${Partition}:iam::${Account}:user/${UserNameWithPath}	aws:ResourceTag/${TagKey} iam:ResourceTag/${TagKey}

Condition keys for Amazon Identity and Access Management (IAM)

Amazon 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 Amazon 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 Amazon service to which this role is attached	String
iam:AssociatedResourceArn	Filters access by the resource that the role will be used on behalf of	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:OrganizationsPolicyId	Filters access by the ID of an Amazon Organizations policy	String

Condition keys	Description	Type
iam:PassedToService	Filters access by the Amazon 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
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

Actions, resources, and condition keys for Amazon Identity and Access Management Roles Anywhere

Amazon 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 Amazon Identity and Access Management Roles Anywhere
- Resource types defined by Amazon Identity and Access Management Roles Anywhere
- Condition keys for Amazon Identity and Access Management Roles Anywhere

Actions defined by Amazon 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 Amazon. 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.

> **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*		
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*		

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			trust-anchor		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a resource	Tagging	crl		
			profile		
			subject		
			trust-anchor		
				aws:TagKeys	
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 Amazon 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 Amazon Identity and Access Management Roles Anywhere

Amazon 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 Amazon 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 Identity Store

Amazon 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 Amazon Identity Store
- Resource types defined by Amazon Identity Store
- Condition keys for Amazon Identity Store

Actions defined by Amazon 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 Amazon. 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.

> **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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateGroupMembership	Grants permission to create a member to a group in the specified IdentityStore	Write	Group*		
			IdentityStore*		
			User*		
CreateUser	Grants permission to create a user in the specified IdentityStore	Write	IdentityStore*		
DeleteGroup	Grants permission to delete a group in the specified IdentityStore	Write	Group*		
			IdentityStore*		
DeleteGroupMembership	Grants permission to remove a member that is part of a group in the specified IdentityStore	Write	Group*		
			GroupMembership*		
			IdentityStore*		
			User*		
DeleteUser	Grants permission to delete a user in the specified IdentityStore	Write	IdentityStore*		
			User*		
DescribeGroup	Grants permission to retrieve information about a group in the specified IdentityStore	Read	Group*		
			IdentityStore*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeGroupMembership	Grants permission to retrieve information about a member that is part of a group in the specified IdentityStore	Read	Group*		
			GroupMembership*		
			Identitystore*		
			User*		
DescribeUser	Grants permission to retrieve information about user in the specified IdentityStore	Read	Identitystore*		
			User*		
GetGroupId	Grants permission to retrieve ID information about group in the specified IdentityStore	Read	Group*		
			Identitystore*		
GetGroupMembershipId	Grants permission to retrieve ID information of a member which is part of a group in the specified IdentityStore	Read	Group*		
			GroupMembership*		
			Identitystore*		
			User*		
GetUserId	Grants permission to retrieves ID information about user in the specified IdentityStore	Read	Identitystore*		
			User*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
IsMemberInGroups	Grants permission to check if a member is a part of groups in the specified IdentityStore	Read	AllGroupMemberships*		
			Group*		
			Identitystore*		
			User*		
ListGroupMemberships	Grants permission to retrieve all members that are part of a group in the specified IdentityStore	List	AllGroupMemberships*		
			Group*		
			Identitystore*		
ListGroupMembershipsForMember	Grants permission to list groups of the target member in the specified IdentityStore	List	AllGroupMemberships*		
			Identitystore*		
			User*		
ListGroups	Grants permission to search for groups within the specified IdentityStore	List	AllGroups*		
			Identitystore*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListUsers	Grants permission to search for users in the specified IdentityStore	List	AllUsers*		
			Identitystore*		
UpdateGroup	Grants permission to update information about a group in the specified IdentityStore	Write	Group*		
			Identitystore*		
UpdateUser	Grants permission to update user information in the specified IdentityStore	Write	Identitystore*		
			User*		

Resource types defined by Amazon 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}`	

Resource types	ARN	Condition keys
Group	`arn:${Partition}:identitystore:::group/${GroupId}`	
GroupMembership	`arn:${Partition}:identitystore:::membership/${MembershipId}`	
AllUsers	`arn:${Partition}:identitystore:::user/*`	
AllGroups	`arn:${Partition}:identitystore:::group/*`	
AllGroupMemberships	`arn:${Partition}:identitystore:::membership/*`	

Condition keys for Amazon Identity Store

Amazon 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 Amazon global condition context keys.

Condition keys	Description	Type
identitystore:UserId	Filters access by IAM Identity Center User ID	String

Actions, resources, and condition keys for Amazon Identity Store Auth

Amazon Identity Store Auth (service prefix: `identitystore-auth`) 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 Identity Store Auth
- Resource types defined by Amazon Identity Store Auth
- Condition keys for Amazon Identity Store Auth

Actions defined by Amazon Identity Store Auth

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 Amazon. 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.

> **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
BatchDeleteSession [permission only]	Grants permission to delete a batch of specified sessions	Write			
BatchGetSession [permission only]	Grants permission to return session attributes for a batch of specified sessions	Read			
ListSessions [permission only]	Grants permission to retrieve a list of active sessions for the specified user	List			

Resource types defined by Amazon Identity Store Auth

Amazon Identity Store Auth does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon Identity Store Auth, specify `"Resource": "*"` in your policy.

Condition keys for Amazon Identity Store Auth

Identity Store Auth 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 Amazon global condition context keys.

Actions, resources, and condition keys for Amazon Identity Sync

Amazon Identity Sync (service prefix: `identity-sync`) 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 Identity Sync
- Resource types defined by Amazon Identity Sync
- Condition keys for Amazon Identity Sync

Actions defined by Amazon Identity Sync

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 Amazon. 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.

> **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	Grants permission to configure vended log delivery for a Sync Profile	Permissions management	SyncProfileResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
[permission only]					
CreateSyncFilter	Grants permission to create a sync filter on the sync profile	Write	SyncProfileResource*		
CreateSyncProfile	Grants permission to create a sync profile for the identity source	Write			ds:AuthorizeApplication
CreateSyncTarget	Grants permission to create a sync target for the identity source	Write	SyncProfileResource*		
DeleteSyncFilter	Grants permission to delete a sync filter from the sync profile	Write	SyncProfileResource*		
DeleteSyncProfile	Grants permission to delete a sync profile from the source	Write	SyncProfileResource*		ds:UnauthorizeApplication
DeleteSyncTarget	Grants permission to delete a sync target from the source	Write	SyncProfileResource*		
			SyncTargetResource*		
GetSyncProfile	Grants permission to retrieve a sync profile by using a sync profile name	Read	SyncProfileResource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSyncTarget	Grants permission to retrieve a sync target from the sync profile	Read	SyncProfileResource*		
			SyncTargetResource*		
ListSyncFilters	Grants permission to list the sync filters from the sync profile	List	SyncProfileResource*		
StartSync	Grants permission to start a sync process or to resume a sync process that was previously paused	Write	SyncProfileResource*		
StopSync	Grants permission to stop any planned sync process in the sync schedule from starting	Write	SyncProfileResource*		
UpdateSyncTarget	Grants permission to update a sync target on the sync profile	Write	SyncProfileResource*		
			SyncTargetResource*		

Resource types defined by Amazon Identity Sync

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
SyncProfileResource	`arn:${Partition}:identity-sync:${Region}:${Account}:profile/${SyncProfileName}`	
SyncTargetResource	`arn:${Partition}:identity-sync:${Region}:${Account}:target/${SyncProfileName}/${SyncTargetName}`	

Condition keys for Amazon Identity Sync

Identity Sync 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 Amazon global condition context keys.

Actions, resources, and condition keys for Amazon Inspector2

Amazon Inspector2 (service prefix: `inspector2`) 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 Inspector2
- Resource types defined by Amazon Inspector2
- Condition keys for Amazon Inspector2

Actions defined by Amazon Inspector2

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 Amazon. 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.

> **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
AssociateMember	Grants permission to associate an account with an Amazon Inspector administrator account	Write			
BatchGetAccountStatus	Grants permission to retrieve information about Amazon Inspector accounts for an account	Read			
BatchGetCodeSnippet	Grants permission to retrieve code snippet information about one or more code vulnerability findings	Read			
BatchGetFindingDetails	Grants permission to let a customer get enhanced vulnerability intelligence details for findings	Read			
BatchGetFreeTrialInfo	Grants permission to retrieve free trial period eligibility about Amazon Inspector accounts for an account	Read			
BatchGetMemberEc2DeepInspectionStatus	Grants permission to delegated administrator to retrieve ec2 deep inspection status of member accounts	Read			
BatchUpdateMemberEc2DeepIns	Grants permission to update ec2 deep inspection status by delegated administrator	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
pectionStatus	for its associated member accounts				
CancelFindingsReport	Grants permission to cancel the generation of a findings report	Write			
CancelSbomExport	Grants permission to cancel the generation of an SBOM report	Write			
CreateCisScanConfiguration	Grants permission to create and define the settings for a CIS scan configuration	Write	CIS Scan Configuration*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateFilter	Grants permission to create and define the settings for a findings filter	Write	Filter*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFindingsReport	Grants permission to request the generation of a findings report	Write			
CreateSbomExport	Grants permission to request the generation of an SBOM report	Write			
DeleteCisScanConfiguration	Grants permission to delete a CIS scan configuration	Write	CIS Scan Configuration*		
				aws:ResourceTag/${TagKey}	
DeleteFilter	Grants permission to delete a findings filter	Write	Filter*		
DescribeOrganizationConfiguration	Grants permission to retrieve information about the Amazon Inspector configuration settings for an Amazon organization	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Disable	Grants permission to disable an Amazon Inspector account	Write			
DisableDelegatedAdminAccount	Grants permission to disable an account as the delegated Amazon Inspector administrator account for an Amazon organization	Write			
DisassociateMember	Grants permission to an Amazon Inspector administrator account to disassociate from an Inspector member account	Write			
Enable	Grants permission to enable and specify the configuration settings for a new Amazon Inspector account	Write			
EnableDelegatedAdminAccount	Grants permission to enable an account as the delegated Amazon Inspector administrator account for an Amazon organization	Write			
GetCisScanReport	Grants permission to retrieve a report containing information about completed CIS scans	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCisScanResultDetails	Grants permission to retrieve information about all details pertaining to one CIS scan and one targeted resource	List			
GetConfiguration	Grants permission to retrieve information about the Amazon Inspector configuration settings for an Amazon Web Services account	Read			
GetDelegatedAdminAccount	Grants permission to retrieve information about the Amazon Inspector administrator account for an account	Read			
GetEc2DeepInspectionConfiguration	Grants permission to retrieve ec2 deep inspection configuration for standalone accounts, delegated administrator and member account	Read			
GetEncryptionKey	Grants permission to retrieve information about the KMS key used to encrypt code snippets with	Read			
GetFindingsReportStatus	Grants permission to retrieve status for a requested findings report	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetMember	Grants permission to retrieve information about an account that's associated with an Amazon Inspector administrator account	Read			
GetSbomExport	Grants permission to retrieve a requested SBOM report	Read			
ListAccountPermissions	Grants permission to retrieve feature configuration permissions associated with an Amazon Inspector account within an organization	List			
ListCisScanConfigurations	Grants permission to retrieve information about all CIS scan configurations	List			
ListCisScanResultsAggregatedByChecks	Grants permission to retrieve information about all checks pertaining to one CIS scan	List			
ListCisScanResultsAggregatedByTargetResource	Grants permission to retrieve information about all resources pertaining to one CIS scan	List			
ListCisScans	Grants permission to retrieve information about completed CIS scans	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListCoverage	Grants permission to retrieve the types of statistics Amazon Inspector can generate for resources Inspector monitors	List			
ListCoverageStatistics	Grants permission to retrieve statistical data and other information about the resources Amazon Inspector monitors	List			
ListDelegatedAdminAccounts	Grants permission to retrieve information about the delegated Amazon Inspector administrator account for an Amazon organization	List			
ListFilters	Grants permission to retrieve information about all findings filters	List			
ListFindingAggregations	Grants permission to retrieve statistical data and other information about Amazon Inspector findings	List			
ListFindings	Grants permission to retrieve a subset of information about one or more findings	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListMembers	Grants permission to retrieve information about the Amazon Inspector member accounts that are associated with an Inspector administrator account	List			
ListTagsForResource	Grants permission to retrieve the tags for an Amazon Inspector resource	Read			
ListUsageTotals	Grants permission to retrieve aggregated usage data for an account	List			
ResetEncryptionKey	Grants permission to let a customer reset to use an Amazon-owned KMS key to encrypt code snippets with	Write			
SearchVulnerabilities	Grants permission to list Amazon Inspector coverage details for a specific vulnerability	Read			
SendCisSessionHealth	Grants permission to send CIS health for a CIS scan	Write			
SendCisSessionTelemetry	Grants permission to send CIS telemetry for a CIS scan	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartCisSession	Grants permission to start a CIS scan session	Write			
StopCisSession	Grants permission to stop a CIS scan session	Write			
TagResource	Grants permission to add or update the tags for an Amazon Inspector resource	Tagging	CIS Scan Configuration	inspector2:CisScanConfiguration	
			Filter	inspector2:Filter	
				aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to remove tags from an Amazon Inspector resource	Tagging	CIS Scan Configuration	inspector2:CisScanConfiguration	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			Filter	inspector2:Filter	
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateCisScanConfiguration	Grants permission to update the settings for a CIS scan configuration	Write	CIS Scan Configuration*		
				aws:ResourceTag/${TagKey}	
UpdateConfiguration	Grants permission to update information about the Amazon Inspector configuration settings for an Amazon Web Services account	Write			
UpdateEc2DeepInspectionConfiguration	Grants permission to update ec2 deep inspection configuration by delegated administrator, member and standalone account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateEncryptionKey	Grants permission to let a customer use a KMS key to encrypt code snippets with	Write			
UpdateFilter	Grants permission to update the settings for a findings filter	Write	Filter*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateOrgEc2DeepInspectionConfiguration	Grants permission to update ec2 deep inspection configuration by delegated administrator for its associated member accounts	Write			
UpdateOrganizationConfiguration	Grants permission to update Amazon Inspector configuration settings for an Amazon organization	Write			

Resource types defined by Amazon Inspector2

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
Filter	`arn:${Partition}:inspector2:${Region}:${Account}:owner/${OwnerId}/filter/${FilterId}`	aws:ResourceTag/${TagKey}
Finding	`arn:${Partition}:inspector2:${Region}:${Account}:finding/${FindingId}`	
CIS Scan Configuration	`arn:${Partition}:inspector2:${Region}:${Account}:owner/${OwnerId}/cis-configuration/${CISScanConfigurationId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Inspector2

Amazon Inspector2 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 Amazon 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 Invoicing Service

Amazon Invoicing Service (service prefix: `invoicing`) 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 Invoicing Service
- Resource types defined by Amazon Invoicing Service
- Condition keys for Amazon Invoicing Service

Actions defined by Amazon Invoicing 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 Amazon. 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.

> **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
BatchGetInvoiceProfile	Grants permission to get invoice profile details for an account in your organization	Read			
CreateInvoiceUnit	Grants permission to create an invoice unit for your organization	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteInvoiceUnit	Grants permission to update an invoice unit for your organization	Write	invoice-unit*		
				aws:ResourceTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey}	
GetInvoiceEmailDeliveryPreferences [permission only]	Grants permission to get Invoice Email Delivery Preferences	Read			
GetInvoicePDF [permission only]	Grants permission to get Invoice PDF	Read			
GetInvoiceUnit	Grants permission to get invoice units for your organization	Read	invoice-unit*		
ListInvoiceSummaries [permission only]	Grants permission to get Invoice summary information for your account or linked account	Read			
ListInvoiceUnits	Grants permission to list invoice units for your organization	List			
ListTagsForResource	Grants permission to list tags for a resource	Read	invoice-unit*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
PutInvoiceEmailDeliveryPreferences [permission only]	Grants permission to put Invoice Email Delivery Preferences	Write			
TagResource	Grants permission to tag a resource	Tagging	invoice-unit*		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to untag a resource	Tagging	invoice-unit*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateInvoiceUnit	Grants permission to update an invoice unit for your organization	Write	invoice-unit*		
				aws:ResourceTag/${TagKey}	

Resource types defined by Amazon Invoicing 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
invoice-unit	`arn:${Partition}:invoicing::${Account}:invoice-unit/${Identifier}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Invoicing Service

Amazon Invoicing 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 Amazon global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by allowed set of values for each of the tags	String
aws:ResourceTag/${TagKey}	Filters access by tag-value associated with the resource	String
aws:TagKeys	Filters access by presence of mandatory tags in the request	ArrayOfString

Actions, resources, and condition keys for Amazon IoT

Amazon IoT (service prefix: `iot`) 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 IoT
- Resource types defined by Amazon IoT
- Condition keys for Amazon IoT

Actions defined by Amazon IoT

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 Amazon. 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.

> **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
AcceptCertificateTransfer	Grants permission to accept a pending certificate transfer	Write	cert*		
AddThingToBillingGroup	Grants permission to add a thing to the specified billing group	Write	billinggroup*		
			thing*		
AddThingToThingGroup	Grants permission to add a thing to the specified thing group	Write	thing*		
			thinggroup*		
AssociateSbomWithPackageVersion	Grants permission to associate SBOM files to a package version	Write	packageversion*		iot:GetIndexingConfiguration
AssociateTargetsWithJob	Grants permission to associate a group with a continuous job	Write	job*		
			thing*		
			thinggroup*		
AttachPolicy	Grants permission to attach a policy to the specified target	Permissions management	cert		
			thinggroup		
AttachPrincipalPolicy	Grants permission to attach the specified policy to the	Permissions	cert		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	specified principal (certificate or other credential)	management			
AttachSecurityProfile	Grants permission to associate a Device Defender security profile with a thing group or with this account	Write	securityprofile*		
			custommetric		
			dimension		
			thinggroup		
AttachThingPrincipal	Grants permission to attach the specified principal to the specified thing	Write	cert		
				iot:thingArn	
CancelAuditMitigationActionsTask	Grants permission to cancel a mitigation action task that is in progress	Write			
CancelAuditTask	Grants permission to cancel an audit that is in progress. The audit can be either scheduled or on-demand	Write			
CancelCertificateTransfer	Grants permission to cancel a pending transfer for the specified certificate	Write	cert*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelDetectMitigationActionsTask	Grants permission to cancel a Device Defender ML Detect mitigation action	Write			
CancelJob	Grants permission to cancel a job	Write	job*		
CancelJobExecution	Grants permission to cancel a job execution on a particular device	Write	job*		
			thing*		
ClearDefaultAuthorizer	Grants permission to clear the default authorizer	Write			
CloseTunnel	Grants permission to close a tunnel	Write	tunnel*		
				iot:Delete	
ConfirmTopicRuleDestination	Grants permission to confirm a http url TopicRuleDestinationDestination	Write	destination*		
Connect	Grants permission to connect as the specified client	Write	client*		
CreateAuditSuppression	Grants permission to create a Device Defender audit suppression	Write			
CreateAuthorizer	Grants permission to create an authorizer	Write	authorizer*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateBillingGroup	Grants permission to create a billing group	Write	billinggroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCertificateFromCsr	Grants permission to create an X.509 certificate using the specified certificate signing request	Write			
CreateCertificateProvider	Grants permission to create a certificate provider	Write	certificateprovider*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCommand	Grants permission to create a command that can be used to start new executions against a device	Write	command*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomMetric	Grants permission to create a custom metric for device side metric reporting and monitoring	Write	custommetric*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDimension	Grants permission to define a dimension that can be used to to limit the scope of a metric used in a security profile	Write	dimension*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDomainConfiguration	Grants permission to create a domain configuration	Write	domainconfiguration*		
				aws:RequestTag/${TagKey} aws:TagKeys iot:DomainName	
CreateDynamicThingGroup	Grants permission to create a Dynamic Thing Group	Write	dynamicthinggroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateFleetMetric	Grants permission to create a fleet metric	Write	fleetmetric*		
			index*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateJob	Grants permission to create a job	Write	job*		
			thing*		
			thinggroup*		
			jobtemplate		
			package		
			packageversion		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateJobTemplate	Grants permission to create a job template	Write	jobtemplate*		
			job		
			package		
			packageversion		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateKeysAndCertificate	Grants permission to create a 2048 bit RSA key pair and issues an X.509 certificate using the issued public key	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateMitigationAction	Grants permission to define an action that can be applied to audit findings by using StartAuditMitigationActions Task	Write	mitigationaction*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateOTAUpdate	Grants permission to create an OTA update job	Write	otaupdate*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePackage	Grants permission to create a software package that you can deploy to your devices	Write	package*		iot:GetIndexingConfiguration
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePackageVersion	Grants permission to create a version under the specified package	Write	package*		iot:GetIndexingConfiguration s3:GetObjectVersion
			packageversion*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePolicy	Grants permission to create an Amazon IoT policy	Write	policy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePolicyVersion	Grants permission to create a new version of the specified Amazon IoT policy	Write	policy*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateProvisioningClaim	Grants permission to create a provisioning claim	Write	provisioningtemplate*		
CreateProvisioningTemplate	Grants permission to create a fleet provisioning template	Write	provisioningtemplate*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateProvisioningTemplateVersion	Grants permission to create a new version of a fleet provisioning template	Write	provisioningtemplate*		
CreateRoleAlias	Grants permission to create a role alias	Write	rolealias*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateScheduledAudit	Grants permission to create a scheduled audit that is run at a specified time interval	Write	scheduledaudit*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSecurityProfile	Grants permission to create a Device Defender security profile	Write	securityprofile*		
			custommetric		
			dimension		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateStream	Grants permission to create a new Amazon IoT stream	Write	stream*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateThing	Grants permission to create a thing in the thing registry	Write	thing*		
			billinggroup		
CreateThingGroup	Grants permission to create a thing group	Write	thinggroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateThingType	Grants permission to create a new thing type	Write	thingtype*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTopicRule	Grants permission to create a rule	Write	rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTopicRuleDestination	Grants permission to create a TopicRuleDestination	Write			
DeleteAccountAuditConfiguration	Grants permission to delete the audit configuration associated with the account	Write			
DeleteAuditSuppression	Grants permission to delete a Device Defender audit suppression	Write			
DeleteAuthorizer	Grants permission to delete the specified authorizer	Write	authorizer*		
DeleteBillingGroup	Grants permission to delete the specified billing group	Write	billinggroup*		
DeleteCACertificate	Grants permission to delete a registered CA certificate	Write	cacert*		
DeleteCertificate	Grants permission to delete the specified certificate	Write	cert*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteCertificateProvider	Grants permission to delete a certificate provider	Write	certificateprovider*		
DeleteCommand	Grants permission to delete a command	Write	command*		
DeleteCommandExecution	Grants permission to delete a command execution	Write	client		
			thing		
DeleteCustomMetric	Grants permission to deletes the specified custom metric from your Amazon Web Services account	Write	custommetric*		
DeleteDimension	Grants permission to remove the specified dimension from your Amazon Web Services account	Write	dimension*		
DeleteDomainConfiguration	Grants permission to delete a domain configuration	Write	domainconfiguration*		
DeleteDynamicThingGroup	Grants permission to delete the specified Dynamic Thing Group	Write	dynamicthinggroup*		
DeleteFleetMetric	Grants permission to delete the specified fleet metric	Write	fleetmetric*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteJob	Grants permission to delete a job and its related job executions	Write	job*		
DeleteJobExecution	Grants permission to delete a job execution	Write	job*		
			thing*		
DeleteJobTemplate	Grants permission to delete a job template	Write	jobtemplate*		
DeleteMitigationAction	Grants permission to delete a defined mitigation action from your Amazon Web Services account	Write	mitigationaction*		
DeleteOTAUpdate	Grants permission to delete an OTA update job	Write	otaupdate*		
DeletePackage	Grants permission to delete a package	Write	package*		
DeletePackageVersion	Grants permission to delete a version of the specified package	Write	package*		
			packageversion*		
DeletePolicy	Grants permission to delete the specified policy	Write	policy*		
DeletePolicyVersion	Grants permission to Delete the specified version of the specified policy	Write	policy*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteProvisioningTemplate	Grants permission to delete a fleet provisioning template	Write	provisioningtemplate*		
DeleteProvisioningTemplateVersion	Grants permission to delete a fleet provisioning template version	Write	provisioningtemplate*		
DeleteRegistrationCode	Grants permission to delete a CA certificate registration code	Write			
DeleteRoleAlias	Grants permission to delete the specified role alias	Write	rolealias*		
DeleteScheduledAudit	Grants permission to delete a scheduled audit	Write	scheduledaudit*		
DeleteSecurityProfile	Grants permission to delete a Device Defender security profile	Write	securityprofile*		
			custommetric		
			dimension		
DeleteStream	Grants permission to delete a specified stream	Write	stream*		
DeleteThing	Grants permission to delete the specified thing	Write	thing*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteThingGroup	Grants permission to delete the specified thing group	Write	thinggroup*		
DeleteThingShadow	Grants permission to delete the specified thing shadow	Write	thing*		
DeleteThingType	Grants permission to delete the specified thing type	Write	thingtype*		
DeleteTopicRule	Grants permission to delete the specified rule	Write	rule*		
DeleteTopicRuleDestination	Grants permission to delete a TopicRuleDestination	Write	destination*		
DeleteV2LoggingLevel	Grants permission to delete the specified v2 logging level	Write			
DeprecateThingType	Grants permission to deprecate the specified thing type	Write	thingtype*		
DescribeAccountAuditConfiguration	Grants permission to get information about audit configurations for the account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeAuditFinding	Grants permission to get information about a single audit finding. Properties include the reason for noncompliance, the severity of the issue, and when the audit that returned the finding was started	Read			
DescribeAuditMitigationActionsTask	Grants permission to get information about an audit mitigation task that is used to apply mitigation actions to a set of audit findings	Read			
DescribeAuditSuppression	Grants permission to get information about a Device Defender audit suppression	Read			
DescribeAuditTask	Grants permission to get information about a Device Defender audit	Read			
DescribeAuthorizer	Grants permission to describe an authorizer	Read	authorizer*		
DescribeBillingGroup	Grants permission to get information about the specified billing group	Read	billinggroup*		
DescribeCACertificate	Grants permission to describe a registered CA certificate	Read	cacert*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeCertificate	Grants permission to get information about the specified certificate	Read	cert*		
DescribeCertificateProvider	Grants permission to describe a certificate provider	Read	certificateprovider*		
DescribeCustomMetric	Grants permission to describe a custom metric that is defined in your Amazon Web Services account	Read	custommetric*		
DescribeDefaultAuthorizer	Grants permission to describe the default authorizer	Read			
DescribeDetectMitigationActionsTask	Grants permission to describe a Device Defender ML Detect mitigation action	Read			
DescribeDimension	Grants permission to get details about a dimension that is defined in your Amazon Web Services account	Read	dimension*		
DescribeDomainConfiguration	Grants permission to get information about the domain configuration	Read	domainconfiguration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeEndpoint	Grants permission to get a unique endpoint specific to the Amazon Web Services account making the call	Read			
DescribeEventConfigurations	Grants permission to get account event configurations	Read			
DescribeFleetMetric	Grants permission to get information about the specified fleet metric	Read	fleetmetric*		
DescribeIndex	Grants permission to get information about the specified index	Read	index*		
DescribeJob	Grants permission to describe a job	Read	job*		
DescribeJobExecution	Grants permission to describe a job execution	Read	job		
			thing		
DescribeJobTemplate	Grants permission to describe a job template	Read	jobtemplate*		
DescribeManagedJobTemplate	Grants permission to describe a managed job template	Read	jobtemplate*		
DescribeMitigationAction	Grants permission to get information about a mitigation action	Read	mitigationaction*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeProvisioningTemplate	Grants permission to get information about a fleet provisioning template	Read	provisioningtemplate*		
DescribeProvisioningTemplateVersion	Grants permission to get information about a fleet provisioning template version	Read	provisioningtemplate*		
DescribeRoleAlias	Grants permission to describe a role alias	Read	rolealias*		
DescribeScheduledAudit	Grants permission to get information about a scheduled audit	Read	scheduledaudit*		
DescribeSecurityProfile	Grants permission to get information about a Device Defender security profile	Read	securityprofile*		
DescribeStream	Grants permission to get information about the specified stream	Read	stream*		
DescribeThing	Grants permission to get information about the specified thing	Read	thing*		
DescribeThingGroup	Grants permission to get information about the specified thing group	Read	thinggroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeThingRegistrationTask	Grants permission to get information about the bulk thing registration task	Read			
DescribeThingType	Grants permission to get information about the specified thing type	Read	thingtype*		
DescribeTunnel	Grants permission to describe a tunnel	Read	tunnel*		
DetachPolicy	Grants permission to detach a policy from the specified target	Permissions management	cert		
			thinggroup		
DetachPrincipalPolicy	Grants permission to remove the specified policy from the specified certificate	Permissions management	cert		
DetachSecurityProfile	Grants permission to disassociate a Device Defender security profile from a thing group or from this account	Write	securityprofile*		
			custommetric		
			dimension		
			thinggroup		
DetachThingPrincipal		Write	cert		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to detach the specified principal from the specified thing			iot:thingArn	
DisableTopicRule	Grants permission to disable the specified rule	Write	rule*		
DisassociateSbomFromPackageVersion	Grants permission to disassociate SBOM files from a package version	Write	packageversion*		
EnableTopicRule	Grants permission to enable the specified rule	Write	rule*		
GetBehaviorModelTrainingSummaries	Grants permission to fetch a Device Defender's ML Detect Security Profile training model's status	List	securityprofile		
GetBucketsAggregation	Grants permission to get buckets aggregation for IoT fleet index	Read	index*		
GetCardinality	Grants permission to get cardinality for IoT fleet index	Read	index*		
GetCommand	Grants permission to get the information about the command	Read	command*		
GetCommandExecution	Grants permission to get the information of a command execution	Read	client		
			thing		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetEffectivePolicies	Grants permission to get effective policies	Read	cert		
GetIndexingConfiguration	Grants permission to get current fleet indexing configuration	Read			
GetJobDocument	Grants permission to get a job document	Read	job*		
GetLoggingOptions	Grants permission to get the logging options	Read			
GetOTAUpdate	Grants permission to get the information about the OTA update job	Read	otaupdate*		
GetPackage	Grants permission to get the information about the package	Read	package*		
GetPackageConfiguration	Grants permission to get the package configuration of the account	Read			
GetPackageVersion	Grants permission to get the version of the package	Read	package*		
			packageversion*		
GetPercentiles	Grants permission to get percentiles for IoT fleet index	Read	index*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetPolicy	Grants permission to get information about the specified policy with the policy document of the default version	Read	policy*		
GetPolicyVersion	Grants permission to get information about the specified policy version	Read	policy*		
GetRegistrationCode	Grants permission to get a registration code used to register a CA certificate with Amazon IoT	Read			
GetRetainedMessage	Grants permission to get the retained message on the specified topic	Read	topic*		
GetStatistics	Grants permission to get statistics for IoT fleet index	Read	index*		
GetThingConnectivityData	Grants permission to get the thing's connectivity data	Read	thing*		
GetThingShadow	Grants permission to get the thing shadow	Read	thing*		
GetTopicRule	Grants permission to get information about the specified rule	Read	rule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTopicRuleDestination	Grants permission to get a TopicRuleDestination	Read	destination*		
GetV2LoggingOptions	Grants permission to get v2 logging options	Read			
ListActiveViolations	Grants permission to list the active violations for a given Device Defender security profile or Thing	List	securityprofile		
			thing		
ListAttachedPolicies	Grants permission to list the policies attached to the specified thing group	List			
ListAuditFindings	Grants permission to list the findings (results) of a Device Defender audit or of the audits performed during a specified time period	List			
ListAuditMitigationActionsExecutions	Grants permission to get the status of audit mitigation action tasks that were executed	List			
ListAuditMitigationActionsTasks	Grants permission to get a list of audit mitigation action tasks that match the specified filters	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAuditSuppressions	Grants permission to list your Device Defender audit suppressions	List			
ListAuditTasks	Grants permission to list the Device Defender audits that have been performed during a given time period	List			
ListAuthorizers	Grants permission to list the authorizers registered in your account	List			
ListBillingGroups	Grants permission to list all billing groups	List			
ListCACertificates	Grants permission to list the CA certificates registered for your Amazon Web Services account	List			
ListCertificateProviders	Grants permission to list certificate providers in the account	List			
ListCertificates	Grants permission to list your certificates	List			
ListCertificatesByCA	Grants permission to list the device certificates signed by the specified CA certificate	List			
ListCommandExecutions		List	client		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to list commands executions in the account		command		
			thing		
ListCommands	Grants permission to list commands in the account	List			
ListCustomMetrics	Grants permission to list the custom metrics in your Amazon Web Services account	List			
ListDetectMitigationActionsExecutions	Grants permission to lists mitigation actions executions for a Device Defender ML Detect Security Profile	List	thing		
ListDetectMitigationActionsTasks	Grants permission to list Device Defender ML Detect mitigation actions tasks	List			
ListDimensions	Grants permission to list the dimensions that are defined for your Amazon Web Services account	List			
ListDomainConfigurations	Grants permission to list the domain configuration created by your Amazon Web Services account	List			
ListFleetMetrics	Grants permission to list the fleet metrics in your account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListIndices	Grants permission to list all indices for fleet index	List			
ListJobExecutionsForJob	Grants permission to list the job executions for a job	List	job*		
ListJobExecutionsForThing	Grants permission to list the job executions for the specified thing	List	thing*		
ListJobTemplates	Grants permission to list job templates	List			
ListJobs	Grants permission to list jobs	List			
ListManagedJobTemplates	Grants permission to list managed job templates	List			
ListMetricValues	Grants permissions to list the metric values for a thing based on the metricName, and dimension if specified	List	thing*		
ListMitigationActions	Grants permission to get a list of all mitigation actions that match the specified filter criteria	List			
ListNamedShadowsForThing	Grants permission to list all named shadows for a given thing	List	thing*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListOTAUpdates	Grants permission to list OTA update jobs in the account	List			
ListOutgoingCertificates	Grants permission to list certificates that are being transfered but not yet accepted	List			
ListPackageVersions	Grants permission to list versions for a package in the account	List			
ListPackages	Grants permission to list packages in the account	List			
ListPolicies	Grants permission to list your policies	List			
ListPolicyPrincipals	Grants permission to list the principals associated with the specified policy	List			
ListPolicyVersions	Grants permission to list the versions of the specified policy, and identifies the default version	List	policy*		
ListPrincipalPolicies	Grants permission to list the policies attached to the specified principal. If you use an Amazon Cognito identity, the ID needs to be in Amazon Cognito Identity format	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPrincipalThings	Grants permission to list the things associated with the specified principal	List	cert		
ListPrincipalThingsV2	Grants permission to list the things associated with the specified principal	List	cert		
ListProvisioningTemplateVersions	Grants permission to get a list of fleet provisioning template versions	List	provisioningtemplate*		
ListProvisioningTemplates	Grants permission to list the fleet provisioning templates in your Amazon Web Services account	List			
ListRelatedResourcesForAuditFinding	Grants permission to list related resources for a single audit finding	List			
ListRetainedMessages	Grants permission to list the retained messages for your account	List			
ListRoleAliases	Grants permission to list role aliases	List			
ListSbomValidationResults	Grants permission to list SBOM validation results of a package version	List	packageversion*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListScheduledAudits	Grants permission to list all of your scheduled audits	List			
ListSecurityProfiles	Grants permission to list the Device Defender security profiles you have created	List	custommetric		
			dimension		
ListSecurityProfilesForTarget	Grants permission to list the Device Defender security profiles attached to a target	List	thinggroup		
ListStreams	Grants permission to list the streams in your account	List			
ListTagsForResource	Grants permission to list all tags for a given resource	Read	authorizer		
			billinggroup		
			cacert		
			certificateprovider		
			command		
			custommetric		
			dimension		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			domainconfiguration		
			dynamicthinggroup		
			fleetmetric		
			job		
			jobtemplate		
			mitigationaction		
			otaupdate		
			policy		
			provisioningtemplate		
			rolealias		
			rule		
			scheduledaudit		
			securityprofile		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			stream		
			thinggroup		
			thingtype		
ListTargetsForPolicy	Grants permission to list targets for the specified policy	List	policy*		
ListTargetsForSecurityProfile	Grants permission to list the targets associated with a given Device Defender security profile	List	securityprofile*		
ListThingGroups	Grants permission to list all thing groups	List			
ListThingGroupsForThing	Grants permission to list thing groups to which the specified thing belongs	List	thing*		
ListThingPrincipals	Grants permission to list the principals associated with the specified thing	List	thing*		
ListThingPrincipalsV2	Grants permission to list the principals associated with the specified thing	List	thing*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListThingRegistrationTaskReports	Grants permission to list information about bulk thing registration tasks	List			
ListThingRegistrationTasks	Grants permission to list bulk thing registration tasks	List			
ListThingTypes	Grants permission to list all thing types	List			
ListThings	Grants permission to list all things	List			
ListThingsInBillingGroup	Grants permission to list all things in the specified billing group	List	billinggroup*		
ListThingsInThingGroup	Grants permission to list all things in the specified thing group	List	thinggroup*		
ListTopicRuleDestinations	Grants permission to list all TopicRuleDestinations	List			
ListTopicRules	Grants permission to list the rules for the specific topic	List			
ListTunnels	Grants permission to list tunnels	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListV2LoggingLevels	Grants permission to list the v2 logging levels	List			
ListViolationEvents	Grants permission to list the Device Defender security profile violations discovered during the given time period	List	securityprofile		
			thing		
OpenTunnel	Grants permission to open a tunnel	Write		aws:RequestTag/${TagKey} aws:TagKeys iot:ThingGroupArn iot:TunnelDestinationService	
Publish	Grants permission to publish to the specified topic	Write	topic*		
PutVerificationStateOnViolation	Grants permission to put verification state on a violation	Write			
Receive	Grants permission to receive from the specified topic	Write	topic*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterCACertificate	Grants permission to register a CA certificate with Amazon IoT	Write		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
RegisterCertificate	Grants permission to register a device certificate with Amazon IoT	Write			
RegisterCertificateWithoutCA	Grants permission to register a device certificate with Amazon IoT without a registered CA (certificate authority)	Write			
RegisterThing	Grants permission to register your thing	Write			
RejectCertificateTransfer	Grants permission to reject a pending certificate transfer	Write	cert*		
RemoveThingFromBillingGroup	Grants permission to remove thing from the specified billing group	Write	billinggroup*		
			thing*		
RemoveThingFromThingGroup	Grants permission to remove thing from the specified thing group	Write	thing*		
			thinggroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ReplaceTopicRule	Grants permission to replace the specified rule	Write	rule*		
RetainPublish	Grants permission to publish a retained message to the specified topic	Write	topic*		
RotateTunnelAccessToken	Grants permission to rotate the access token of a tunnel	Write	tunnel*		
				iot:ThingGroupArn iot:TunnelDestinationService iot:ClientMode	
SearchIndex	Grants permission to search IoT fleet index	Read	index*		
SetDefaultAuthorizer	Grants permission to set the default authorizer. This will be used if a websocket connection is made without specifying an authorizer	Permissions management	authorizer*		
SetDefaultPolicyVersion	Grants permission to set the specified version of the specified policy as the policy's default (operative) version	Permissions management	policy*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SetLoggingOptions	Grants permission to set the logging options	Write			
SetV2LoggingLevel	Grants permission to set the v2 logging level	Write			
SetV2LoggingOptions	Grants permission to set the v2 logging options	Write			
StartAuditMitigationActionsTask	Grants permission to start a task that applies a set of mitigation actions to the specified target	Write			
StartCommandExecution	Grants permission to start a new command execution	Write	command*		
			client		
			thing		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				iot:CommandExecutionParameterString/${CommandParameterName} iot:CommandExecutionParameterBoolean/${CommandParameterName} iot:CommandExecutionParameterNumber/${CommandParameterName}	
StartDetectMitigationActionsTask	Grants permission to start a Device Defender ML Detect mitigation actions task	Write	securityprofile		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartOnDemandAuditTask	Grants permission to start an on-demand Device Defender audit	Write			
StartThingRegistrationTask	Grants permission to start a bulk thing registration task	Write			
StopThingRegistrationTask	Grants permission to stop a bulk thing registration task	Write			
Subscribe	Grants permission to subscribe to the specified TopicFilter	Write	topicfilter*		
TagResource	Grants permission to tag a specified resource	Tagging	authorizer		
			billinggroup		
			cacert		
			certificateprovider		
			command		
			custommetric		
			dimension		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			domainconfiguration		
			dynamicthinggroup		
			fleetmetric		
			job		
			jobtemplate		
			mitigationaction		
			otaupdate		
			package		
			packageversion		
			policy		
			provisioningtemplate		
			rolealias		
			rule		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			scheduledaudit		
			securityprofile		
			stream		
			thinggroup		
			thingtype		
				aws:RequestTag/${TagKey} aws:TagKeys	
TestAuthorization	Grants permission to test the policies evaluation for group policies	Read	cert		
TestInvokeAuthorizer	Grants permission to test invoke the specified custom authorizer for testing purposes	Read	authorizer*		
TransferCertificate	Grants permission to transfer the specified certificate to the specified Amazon Web Services account	Write	cert*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagResource	Grants permission to untag a specified resource	Tagging	authorizer		
			billinggroup		
			cacert		
			certificateprovider		
			command		
			custommetric		
			dimension		
			domainconfiguration		
			dynamicthinggroup		
			fleetmetric		
			job		
			jobtemplate		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			mitigationaction		
			otaupdate		
			package		
			packageversion		
			policy		
			provisioningtemplate		
			rolealias		
			rule		
			scheduledaudit		
			securityprofile		
			stream		
			thinggroup		
			thingtype		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAccountAuditConfiguration	Grants permission to configure or reconfigure the Device Defender audit settings for this account	Write			
UpdateAuditSuppression	Grants permission to update a Device Defender audit suppression	Write			
UpdateAuthorizer	Grants permission to update an authorizer	Write	authorizer*		
UpdateBillingGroup	Grants permission to update information associated with the specified billing group	Write	billinggroup*		
UpdateCACertificate	Grants permission to update a registered CA certificate	Write	cacert*		iam:PassRole
UpdateCertificate	Grants permission to update the status of the specified certificate. This operation is idempotent	Write	cert*		
UpdateCertificateProvider	Grants permission to update a certificate provider	Write	certificateprovider*		
UpdateCommand	Grants permission to update a command	Write	command*		
UpdateCustomMetric	Grants permission to update the specified custom metric	Write	custommetric*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateDimension	Grants permission to update the definition for a dimension	Write	dimension*		
UpdateDomainConfiguration	Grants permission to update a domain configuration	Write	domainconfiguration*		
UpdateDynamicThingGroup	Grants permission to update a Dynamic Thing Group	Write	dynamicthinggroup*		
UpdateEventConfigurations	Grants permission to update event configurations	Write			
UpdateFleetMetric	Grants permission to update a fleet metric	Write	fleetmetric*		
			index*		
UpdateIndexingConfiguration	Grants permission to update fleet indexing configuration	Write			
UpdateJob	Grants permission to update a job	Write	job*		
UpdateMitigationAction	Grants permission to update the definition for the specified mitigation action	Write	mitigationaction*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdatePackage	Grants permission to update a package	Write	package*		iot:GetIndexingConfiguration
UpdatePackageConfiguration	Grants permission to update the package configuration of the account	Write			iam:PassRole
UpdatePackageVersion	Grants permission to update the version of the specified package	Write	package*		iot:GetIndexingConfiguration s3:GetObjectVersion
			packageversion*		
UpdateProvisioningTemplate	Grants permission to update a fleet provisioning template	Write	provisioningtemplate*		iam:PassRole
UpdateRoleAlias	Grants permission to update the role alias	Write	rolealias*		iam:PassRole
UpdateScheduledAudit	Grants permission to update a scheduled audit, including what checks are performed and how often the audit takes place	Write	scheduledaudit*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateSecurityProfile	Grants permission to update a Device Defender security profile	Write	securityprofile*		
			custommetric		
			dimension		
UpdateStream	Grants permission to update the data for a stream	Write	stream*		
UpdateThing	Grants permission to update information associated with the specified thing	Write	thing*		
UpdateThingGroup	Grants permission to update information associated with the specified thing group	Write	thinggroup*		
UpdateThingGroupsForThing	Grants permission to update the thing groups to which the thing belongs	Write	thing*		
			thinggroup		
UpdateThingShadow	Grants permission to update the thing shadow	Write	thing*		
UpdateThingType	Grants permission to update information associated with the specified thing type	Write	thingtype*		
UpdateTopicRuleDestination	Grants permission to update a TopicRuleDestination	Write	destination*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ValidateSecurityProfileBehaviors	Grants permission to validate a Device Defender security profile behaviors specification	Read			

Resource types defined by Amazon IoT

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
client	`arn:${Partition}:iot:${Region}:${Account}:client/${ClientId}`	
index	`arn:${Partition}:iot:${Region}:${Account}:index/${IndexName}`	
fleetmetric	`arn:${Partition}:iot:${Region}:${Account}:fleetmetric/${FleetMetricName}`	aws:ResourceTag/${TagKey}
job	`arn:${Partition}:iot:${Region}:${Account}:job/${JobId}`	aws:ResourceTag/${TagKey}
jobtemplate	`arn:${Partition}:iot:${Region}:${Account}:jobtemplate/${JobTemplateId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
tunnel	arn:${Partition}:iot:${Region}:${Account}:tunnel/${TunnelId}	aws:ResourceTag/${TagKey}
thing	arn:${Partition}:iot:${Region}:${Account}:thing/${ThingName}	
thinggroup	arn:${Partition}:iot:${Region}:${Account}:thinggroup/${ThingGroupName}	aws:ResourceTag/${TagKey}
billinggroup	arn:${Partition}:iot:${Region}:${Account}:billinggroup/${BillingGroupName}	aws:ResourceTag/${TagKey}
dynamicthinggroup	arn:${Partition}:iot:${Region}:${Account}:thinggroup/${ThingGroupName}	aws:ResourceTag/${TagKey}
thingtype	arn:${Partition}:iot:${Region}:${Account}:thingtype/${ThingTypeName}	aws:ResourceTag/${TagKey}
topic	arn:${Partition}:iot:${Region}:${Account}:topic/${TopicName}	
topicfilter	arn:${Partition}:iot:${Region}:${Account}:topicfilter/${TopicFilter}	
rolealias	arn:${Partition}:iot:${Region}:${Account}:rolealias/${RoleAlias}	aws:ResourceTag/${TagKey}
authorizer	arn:${Partition}:iot:${Region}:${Account}:authorizer/${AuthorizerName}	aws:ResourceTag/${TagKey}
policy	arn:${Partition}:iot:${Region}:${Account}:policy/${PolicyName}	aws:ResourceTag/${TagKey}
cert	arn:${Partition}:iot:${Region}:${Account}:cert/${Certificate}	

Resource types	ARN	Condition keys
cacert	arn:${Partition}:iot:${Region}:${Account}:cacert/${CACertificate}	aws:ResourceTag/${TagKey}
stream	arn:${Partition}:iot:${Region}:${Account}:stream/${StreamId}	aws:ResourceTag/${TagKey}
otaupdate	arn:${Partition}:iot:${Region}:${Account}:otaupdate/${OtaUpdateId}	aws:ResourceTag/${TagKey}
scheduled audit	arn:${Partition}:iot:${Region}:${Account}:scheduledaudit/${ScheduleName}	aws:ResourceTag/${TagKey}
mitigationaction	arn:${Partition}:iot:${Region}:${Account}:mitigationaction/${MitigationActionName}	aws:ResourceTag/${TagKey}
securityprofile	arn:${Partition}:iot:${Region}:${Account}:securityprofile/${SecurityProfileName}	aws:ResourceTag/${TagKey}
custommetric	arn:${Partition}:iot:${Region}:${Account}:custommetric/${MetricName}	aws:ResourceTag/${TagKey}
dimension	arn:${Partition}:iot:${Region}:${Account}:dimension/${DimensionName}	aws:ResourceTag/${TagKey}
rule	arn:${Partition}:iot:${Region}:${Account}:rule/${RuleName}	aws:ResourceTag/${TagKey}
destination	arn:${Partition}:iot:${Region}:${Account}:ruledestination/${DestinationType}/${Uuid}	
provisioningtemplate	arn:${Partition}:iot:${Region}:${Account}:provisioningtemplate/${ProvisioningTemplate}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
domainconfiguration	`arn:${Partition}:iot:${Region}:${Account}:domainconfiguration/${DomainConfigurationName}/${Id}`	aws:ResourceTag/${TagKey}
package	`arn:${Partition}:iot:${Region}:${Account}:package/${PackageName}`	aws:ResourceTag/${TagKey}
packageversion	`arn:${Partition}:iot:${Region}:${Account}:package/${PackageName}/version/${VersionName}`	aws:ResourceTag/${TagKey}
certificateprovider	`arn:${Partition}:iot:${Region}:${Account}:certificateprovider/${CertificateProviderName}`	aws:ResourceTag/${TagKey}
command	`arn:${Partition}:iot:${Region}:${Account}:command/${CommandId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon IoT

Amazon IoT 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 Amazon global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag key that is present in the request	String
aws:ResourceTag/${TagKey}	Filters access by a tag key component of a tag associated to the IoT resource in the request	String

Condition keys	Description	Type
aws:TagKeys	Filters access by a list of tag keys associated to the IoT resource in the request	ArrayOfString
iot:ClientMode	Filters access by the mode of the client for IoT Tunnel	String
iot:CommandExecutionParameterBoolean/${CommandParameterName}	Filters access by the command parameter name and boolean value	Bool
iot:CommandExecutionParameterNumber/${CommandParameterName}	Filters access by the command parameter name and numeric value	Numeric
iot:CommandExecutionParameterString/${CommandParameterName}	Filters access by the command parameter name and string value	String
iot:Delete	Filters access by a flag indicating whether or not to also delete an IoT Tunnel immediately when making iot:CloseTunnel request	Bool
iot:DomainName	Filters access by based on the domain name of an IoT DomainConfiguration	String

Condition keys	Description	Type
iot:ThingGroupArn	Filters access by a list of IoT Thing Group ARNs that the destination IoT Thing belongs to for an IoT Tunnel	ArrayOfARN
iot:TunnelDestinationService	Filters access by a list of destination services for an IoT Tunnel	ArrayOfString
iot:thingArn	Filters access by the ARN of an IoT Thing	ARN

Actions, resources, and condition keys for Amazon IoT Analytics

Amazon IoT Analytics (service prefix: `iotanalytics`) 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 IoT Analytics
- Resource types defined by Amazon IoT Analytics
- Condition keys for Amazon IoT Analytics

Actions defined by Amazon IoT Analytics

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 Amazon. 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.

> **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
BatchPutMessage	Puts a batch of messages into the specified channel	Write	channel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelPipelineReprocessing	Cancels reprocessing for the specified pipeline	Write	pipeline*		
CreateChannel	Creates a channel	Write	channel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataset	Creates a dataset	Write	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDatasetContent	Generates content from the specified dataset (by executing the dataset actions)	Write	dataset*		
CreateDatastore	Creates a datastore	Write	datastore*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePipeline	Creates a pipeline	Write	pipeline*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteChannel	Deletes the specified channel	Write	channel*		
DeleteDataset	Deletes the specified dataset	Write	dataset*		
DeleteDatasetContent	Deletes the content of the specified dataset	Write	dataset*		
DeleteDatastore	Deletes the specified datastore	Write	datastore*		
DeletePipeline	Deletes the specified pipeline	Write	pipeline*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeChannel	Describes the specified channel	Read	channel*		
DescribeDataset	Describes the specified dataset	Read	dataset*		
DescribeDatastore	Describes the specified datastore	Read	datastore*		
DescribeLoggingOptions	Describes logging options for the the account	Read			
DescribePipeline	Describes the specified pipeline	Read	pipeline*		
GetDatasetContent	Gets the content of the specified dataset	Read	dataset*		
ListChannels	Lists the channels for the account	List			
ListDatasetContents	Lists information about dataset contents that have been created	List	dataset*		
ListDatasets	Lists the datasets for the account	List			
ListDatastores	Lists the datastores for the account	List			
ListPipelines	Lists the pipelines for the account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Lists the tags (metadata) which you have assigned to the resource	Read	channel		
			dataset		
			datastore		
			pipeline		
PutLoggingOptions	Puts logging options for the the account	Write			
RunPipelineActivity	Runs the specified pipeline activity	Read			
SampleChannelData	Samples the specified channel's data	Read	channel*		
StartPipelineReprocessing	Starts reprocessing for the specified pipeline	Write	pipeline*		
TagResource	Adds to or modifies the tags of the given resource. Tags are metadata which can be used to manage a resource	Tagging	channel		
			dataset		
			datastore		
			pipeline		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Removes the given tags (metadata) from the resource	Tagging	channel		
			dataset		
			datastore		
			pipeline		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateChannel	Updates the specified channel	Write	channel*		
UpdateDataset	Updates the specified dataset	Write	dataset*		
UpdateDatastore	Updates the specified datastore	Write	datastore*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdatePipeline	Updates the specified pipeline	Write	pipeline*		

Resource types defined by Amazon IoT Analytics

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
channel	`arn:${Partition}:iotanalytics:${Region}:${Account}:channel/${ChannelName}`	aws:RequestTag/${TagKey} aws:TagKeys iotanalytics:ResourceTag/${TagKey}
dataset	`arn:${Partition}:iotanalytics:${Region}:${Account}:dataset/${DatasetName}`	aws:RequestTag/${TagKey} aws:TagKeys iotanalytics:ResourceTag/${TagKey}
datastore	`arn:${Partition}:iotanalytics:${Region}:${Account}:datastore/${DatastoreName}`	aws:RequestTag/${TagKey}

Resource types	ARN	Condition keys
		aws:TagKeys iotanalytics:ResourceTag/${TagKey}
pipeline	`arn:${Partition}:iotanalytics:${Region}:${Account}:pipeline/${PipelineName}`	aws:RequestTag/${TagKey} aws:TagKeys iotanalytics:ResourceTag/${TagKey}

Condition keys for Amazon IoT Analytics

Amazon IoT Analytics 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 Amazon global condition context keys.

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

Actions, resources, and condition keys for Amazon IoT Events

Amazon IoT Events (service prefix: `iotevents`) 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 IoT Events
- Resource types defined by Amazon IoT Events
- Condition keys for Amazon IoT Events

Actions defined by Amazon IoT Events

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 Amazon. 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.

> **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
BatchAcknowledgeAlarm	Grants permission to send one or more acknowledge action requests to Amazon IoT Events	Write	alarmModel*		
BatchDeleteDetector	Grants permission to delete a detector instance within the Amazon IoT Events system	Write	detectorModel*		
BatchDisableAlarm	Grants permission to disable one or more alarm instances	Write	alarmModel*		
BatchEnableAlarm	Grants permission to enable one or more alarm instances	Write	alarmModel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchPutMessage	Grants permission to send a set of messages to the Amazon IoT Events system	Write	input*		
BatchResetAlarm	Grants permission to reset one or more alarm instances	Write	alarmModel*		
BatchSnoozeAlarm	Grants permission to change one or more alarm instances to the snooze mode	Write	alarmModel*		
BatchUpdateDetector	Grants permission to update a detector instance within the Amazon IoT Events system	Write	detectorModel*		
CreateAlarmModel	Grants permission to create an alarm model to monitor an Amazon IoT Events input attribute or an Amazon IoT SiteWise asset property	Write	alarmModel*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDetectorModel	Grants permission to create a detector model to monitor an Amazon IoT Events input attribute	Write	detectorModel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInput	Grants permission to create an Input in IotEvents	Write	input*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAlarmModel	Grants permission to delete an alarm model	Write	alarmModel*		
DeleteDetectorModel	Grants permission to delete a detector model	Write	detectorModel*		
DeleteInput	Grants permission to delete an input	Write	input*		
DescribeAlarm	Grants permission to retrieve information about an alarm instance	Read	alarmModel*		
DescribeAlarmModel	Grants permission to retrieve information about an alarm model	Read	alarmModel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDetector	Grants permission to retriev information about a detector instance	Read	detectorModel*		
DescribeDetectorModel	Grants permission to retrieve information about a detector model	Read	detectorModel*		
DescribeDetectorModelAnalysis	Grants permission to retrieve the detector model analysis information	Read			
DescribeInput	Grants permission to retrieve an information about Input	Read	input*		
DescribeLoggingOptions	Grants permission to retrieve the current settings of the Amazon IoT Events logging options	Read			
GetDetectorModelAnalysisResults	Grants permission to retrieve the detector model analysis results	Read			
ListAlarmModelVersions	Grants permission to list all the versions of an alarm model	List	alarmModel*		
ListAlarmModels	Grants permission to list the alarm models that you created	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAlarms	Grants permission to retrieve information about all alarm instances per alarmModel	List	alarmModel*		
ListDetectorModelVersions	Grants permission to list all the versions of a detector model	List	detectorModel*		
ListDetectorModels	Grants permission to list the detector models that you created	List			
ListDetectors	Grants permission to retrieve information about all detector instances per detectormodel	List	detectorModel*		
ListInputRoutings	Grants permission to list one or more input routings	List			
ListInputs	Grants permission to lists the inputs you have created	List			
ListTagsForResource	Grants permission to list the tags (metadata) which you have assigned to the resource	Read	alarmModel		
			detectorModel		
			input		
PutLoggingOptions	Grants permission to set or update the Amazon IoT Events logging options	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartDetectorModelAnalysis	Grants permission to start the detector model analysis	Write			
TagResource	Grants permission to adds to or modifies the tags of the given resource.Tags are metadata which can be used to manage a resource	Tagging	alarmModel		
			detectorModel		
			input		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove the given tags (metadata) from the resource	Tagging	alarmModel		
			detectorModel		
			input		
				aws:TagKeys	
UpdateAlarmModel	Grants permission to update an alarm model	Write	alarmModel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateDetectorModel	Grants permission to update a detector model	Write	detectorModel*		
UpdateInput	Grants permission to update an input	Write	input*		
UpdateInputRouting	Grants permission to update input routing	Write	input*		

Resource types defined by Amazon IoT Events

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
detectorModel	`arn:${Partition}:iotevents:${Region}:${Account}:detectorModel/${DetectorModelName}`	aws:ResourceTag/${TagKey}
alarmModel	`arn:${Partition}:iotevents:${Region}:${Account}:alarmModel/${AlarmModelName}`	aws:ResourceTag/${TagKey}
input	`arn:${Partition}:iotevents:${Region}:${Account}:input/${InputName}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon IoT Events

Amazon IoT Events 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 Amazon 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 actions by the tag keys in the request	ArrayOfString
iotevents:keyValue	Filters access by the instanceId (key-value) of the message	String

Actions, resources, and condition keys for Amazon IoT Greengrass

Amazon IoT Greengrass (service prefix: `greengrass`) 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 IoT Greengrass

- Resource types defined by Amazon IoT Greengrass
- Condition keys for Amazon IoT Greengrass

Actions defined by Amazon IoT Greengrass

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 Amazon. 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.

> **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
AssociateRoleToGroup	Grants permission to associate a role with a group. The role's permissions must allow Greengrass core Lambda functions and connectors to perform actions in other Amazon services	Write	group*		
AssociateServiceRoleToAccount	Grants permission to associate a role with your account. Amazon IoT Greengrass uses this role to access your Lambda functions and Amazon IoT resources	Permissions management			
CreateConnectorDefinition	Grants permission to create a connector definition	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateConnectorDefinitionVersion	Grants permission to create a version of an existing connector definition	Write	connectorDefinition*		
CreateCoreDefinition	Grants permission to create a core definition	Write		aws:RequestTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} aws:TagKeys	
CreateCoreDefinitionVersion	Grants permission to create a version of an existing core definition. Greengrass groups must each contain exactly one Greengrass core	Write	coreDefinition*		
CreateDeployment	Grants permission to create a deployment	Write	group*		
CreateDeviceDefinition	Grants permission to create a device definition	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateDeviceDefinitionVersion	Grants permission to create a version of an existing device definition	Write	deviceDefinition*		
CreateFunctionDefinition	Grants permission to create a Lambda function definition to be used in a group that contains a list of Lambda functions and their configurations	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateFunctionDefinitionVersion	Grants permission to create a version of an existing Lambda function definition	Write	functionDefinition*		
CreateGroup	Grants permission to create a group	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateGroupCertificateAuthority	Grants permission to create a CA for the group, or rotate the existing CA	Write	group*		
CreateGroupVersion	Grants permission to create a version of a group that has already been defined	Write	group*		
CreateLoggerDefinition	Grants permission to create a logger definition	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLoggerDefinitionVersion	Grants permission to create a version of an existing logger definition	Write	loggerDefinition*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateResourceDefinition	Grants permission to create a resource definition that contains a list of resources to be used in a group	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateResourceDefinitionVersion	Grants permission to create a version of an existing resource definition	Write	resourceDefinition*		
CreateSoftwareUpdateJob	Grants permission to create an Amazon IoT job that will trigger your Greengrass cores to update the software they are running	Write			
CreateSubscriptionDefinition	Grants permission to create a subscription definition	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubscriptionDefinitionVersion	Grants permission to create a version of an existing subscription definition	Write	subscriptionDefinition*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteConnectorDefinition	Grants permission to delete a connector definition	Write	connectorDefinition*		
DeleteCoreDefinition	Grants permission to delete a core definition. Deleting a definition that is currently in use in a deployment affects future deployments	Write	coreDefinition*		
DeleteDeviceDefinition	Grants permission to delete a device definition. Deleting a definition that is currently in use in a deployment affects future deployments	Write	deviceDefinition*		
DeleteFunctionDefinition	Grants permission to delete a Lambda function definition. Deleting a definition that is currently in use in a deployment affects future deployments	Write	functionDefinition*		
DeleteGroup	Grants permission to delete a group that is not currently in use in a deployment	Write	group*		
DeleteLoggerDefinition	Grants permission to delete a logger definition. Deleting a definition that is currently in use in a deployment affects future deployments	Write	loggerDefinition*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteResourceDefinition	Grants permission to delete a resource definition	Write	resourceDefinition*		
DeleteSubscriptionDefinition	Grants permission to delete a subscription definition. Deleting a definition that is currently in use in a deployment affects future deployments	Write	subscriptionDefinition*		
DisassociateRoleFromGroup	Grants permission to disassociate the role from a group	Write	group*		
DisassociateServiceRoleFromAccount	Grants permission to disassociate the service role from an account. Without a service role, deployments will not work	Write			
Discover	Grants permission to retrieve information required to connect to a Greengrass core	Read	thing*		
GetAssociatedRole	Grants permission to retrieve the role associated with a group	Read	group*		
GetBulkDeploymentStatus	Grants permission to return the status of a bulk deployment	Read	bulkDeployment*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetConnectivityInfo	Grants permission to retrieve the connectivity information for a core	Read	connectivityInfo*		
GetConnectorDefinition	Grants permission to retrieve information about a connector definition	Read	connectorDefinition*		
GetConnectorDefinitionVersion	Grants permission to retrieve information about a connector definition version	Read	connectorDefinition*		
			connectorDefinitionVersion*		
GetCoreDefinition	Grants permission to retrieve information about a core definition	Read	coreDefinition*		
GetCoreDefinitionVersion	Grants permission to retrieve information about a core definition version	Read	coreDefinition*		
			coreDefinitionVersion*		
GetDeploymentStatus	Grants permission to return the status of a deployment	Read	deployment*		
			group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDeviceDefinition	Grants permission to retrieve information about a device definition	Read	deviceDefinition*		
GetDeviceDefinitionVersion	Grants permission to retrieve information about a device definition version	Read	deviceDefinition*		
			deviceDefinitionVersion*		
GetFunctionDefinition	Grants permission to retrieve information about a Lambda function definition, such as its creation time and latest version	Read	functionDefinition*		
GetFunctionDefinitionVersion	Grants permission to retrieve information about a Lambda function definition version, such as which Lambda functions are included in the version and their configurations	Read	functionDefinition*		
			functionDefinitionVersion*		
GetGroup	Grants permission to retrieve information about a group	Read	group*		
GetGroupCertificateAuthority	Grants permission to return the public key of the CA associated with a group	Read	certificateAuthority*		
			group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetGroupCertificateConfiguration	Grants permission to retrieve the current configuration for the CA used by a group	Read	group*		
GetGroupVersion	Grants permission to retrieve information about a group version	Read	group*		
			groupVersion*		
GetLoggerDefinition	Grants permission to retrieve information about a logger definition	Read	loggerDefinition*		
GetLoggerDefinitionVersion	Grants permission to retrieve information about a logger definition version	Read	loggerDefinition*		
			loggerDefinitionVersion*		
GetResourceDefinition	Grants permission to retrieve information about a resource definition, such as its creation time and latest version	Read	resourceDefinition*		
GetResourceDefinitionVersion	Grants permission to retrieve information about a resource definition version, such as which resources are included in the version	Read	resourceDefinition*		
			resourceDefinitionVersion*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetServiceRoleForAccount	Grants permission to retrieve the service role that is attached to an account	Read			
GetSubscriptionDefinition	Grants permission to retrieve information about a subscription definition	Read	subscriptionDefinition*		
GetSubscriptionDefinitionVersion	Grants permission to retrieve information about a subscription definition version	Read	subscriptionDefinition*		
			subscriptionDefinitionVersion*		
GetThingRuntimeConfiguration	Grants permission to retrieve runtime configuration of a thing	Read	thingRuntimeConfig*		
ListBulkDeploymentDetailedReports	Grants permission to retrieve a paginated list of the deployments that have been started in a bulk deployment operation and their current deployment status	Read	bulkDeployment*		
ListBulkDeployments	Grants permission to retrieve a list of bulk deployments	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListConnectorDefinitionVersions	Grants permission to list the versions of a connector definition	List	connectorDefinition*		
ListConnectorDefinitions	Grants permission to retrieve a list of connector definitions	List			
ListCoreDefinitionVersions	Grants permission to list the versions of a core definition	List	coreDefinition*		
ListCoreDefinitions	Grants permission to retrieve a list of core definitions	List			
ListDeployments	Grants permission to retrieve a list of all deployments for a group	List	group*		
ListDeviceDefinitionVersions	Grants permission to list the versions of a device definition	List	deviceDefinition*		
ListDeviceDefinitions	Grants permission to retrieve a list of device definitions	List			
ListFunctionDefinitionVersions	Grants permission to list the versions of a Lambda function definition	List	functionDefinition*		
ListFunctionDefinitions	Grants permission to retrieve a list of Lambda function definitions	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListGroupCertificateAuthorities	Grants permission to retrieve a list of current CAs for a group	List	group*		
ListGroupVersions	Grants permission to list the versions of a group	List	group*		
ListGroups	Grants permission to retrieve a list of groups	List			
ListLoggerDefinitionVersions	Grants permission to list the versions of a logger definition	List	loggerDefinition*		
ListLoggerDefinitions	Grants permission to retrieve a list of logger definitions	List			
ListResourceDefinitionVersions	Grants permission to list the versions of a resource definition	List	resourceDefinition*		
ListResourceDefinitions	Grants permission to retrieve a list of resource definitions	List			
ListSubscriptionDefinitionVersions	Grants permission to list the versions of a subscription definition	List	subscriptionDefinition*		
ListSubscriptionDefinitions	Grants permission to retrieve a list of subscription definitions	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to list the tags for a resource	Read	bulkDeployment		
			connectorDefinition		
			coreDefinition		
			deviceDefinition		
			functionDefinition		
			group		
			loggerDefinition		
			resourceDefinition		
			subscriptionDefinition		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
ResetDeployments	Grants permission to reset a group's deployments	Write	group*		
StartBulkDeployment	Grants permission to deploy multiple groups in one operation	Write		aws:RequestTag/${TagKey} aws:TagKeys	
StopBulkDeployment	Grants permission to stop the execution of a bulk deployment	Write	bulkDeployment*		
TagResource	Grants permission to add tags to a resource	Tagging	bulkDeployment		
			connectorDefinition		
			coreDefinition		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			deviceDefinition		
			functionDefinition		
			group		
			loggerDefinition		
			resourceDefinition		
			subscriptionDefinition		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from a resource	Tagging	bulkDeployment		
			connectorDefinition		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			coreDefinition		
			deviceDefinition		
			functionDefinition		
			group		
			loggerDefinition		
			resourceDefinition		
			subscriptionDefinition		
				aws:TagKeys	
UpdateConnectivityInfo	Grants permission to update the connectivity information for a Greengrass core. Any devices that belong to the group that has this core will receive this information in order to find the location of the core and connect to it	Write	connectivityInfo*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateConnectorDefinition	Grants permission to update a connector definition	Write	connectorDefinition*		
UpdateCoreDefinition	Grants permission to update a core definition	Write	coreDefinition*		
UpdateDeviceDefinition	Grants permission to update a device definition	Write	deviceDefinition*		
UpdateFunctionDefinition	Grants permission to update a Lambda function definition	Write	functionDefinition*		
UpdateGroup	Grants permission to update a group	Write	group*		
UpdateGroupCertificateConfiguration	Grants permission to update the certificate expiry time for a group	Write	group*		
UpdateLoggerDefinition	Grants permission to update a logger definition	Write	loggerDefinition*		
UpdateResourceDefinition	Grants permission to update a resource definition	Write	resourceDefinition*		
UpdateSubscriptionDefinition	Grants permission to update a subscription definition	Write	subscriptionDefinition*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateThingRuntimeConfiguration	Grants permission to update runtime configuration of a thing	Write	thingRuntimeConfig*		

Resource types defined by Amazon IoT Greengrass

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
connectivityInfo	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/things/${ThingName}/connectivityInfo`	
certificateAuthority	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/groups/${GroupId}/certificateauthorities/${CertificateAuthorityId}`	
deployment	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/groups/${GroupId}/deployments/${DeploymentId}`	
bulkDeployment	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/bulk/deployments/${BulkDeploymentId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
group	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/groups/${GroupId}	aws:ResourceTag/${TagKey}
groupVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/groups/${GroupId}/versions/${VersionId}	
coreDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/cores/${CoreDefinitionId}	aws:ResourceTag/${TagKey}
coreDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/cores/${CoreDefinitionId}/versions/${VersionId}	
deviceDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/devices/${DeviceDefinitionId}	aws:ResourceTag/${TagKey}
deviceDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/devices/${DeviceDefinitionId}/versions/${VersionId}	
functionDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/functions/${FunctionDefinitionId}	aws:ResourceTag/${TagKey}
functionDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/functions/${FunctionDefinitionId}/versions/${VersionId}	

Resource types	ARN	Condition keys
subscriptionDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/subscriptions/${SubscriptionDefinitionId}	aws:ResourceTag/${TagKey}
subscriptionDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/subscriptions/${SubscriptionDefinitionId}/versions/${VersionId}	
loggerDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/loggers/${LoggerDefinitionId}	aws:ResourceTag/${TagKey}
loggerDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/loggers/${LoggerDefinitionId}/versions/${VersionId}	
resourceDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/resources/${ResourceDefinitionId}	aws:ResourceTag/${TagKey}
resourceDefinitionVersion	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/resources/${ResourceDefinitionId}/versions/${VersionId}	
connectorDefinition	arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/connectors/${ConnectorDefinitionId}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
connectorDefinitionVersion	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/definition/connectors/${ConnectorDefinitionId}/versions/${VersionId}`	
thing	`arn:${Partition}:iot:${Region}:${Account}:thing/${ThingName}`	
thingRuntimeConfig	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/things/${ThingName}/runtimeconfig`	

Condition keys for Amazon IoT Greengrass

Amazon IoT Greengrass 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 Amazon global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the allowed set of values for each of the mandatory tags	String
aws:ResourceTag/${TagKey}	Filters access by the 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 Amazon IoT Greengrass V2

Amazon IoT Greengrass V2 (service prefix: `greengrass`) 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 IoT Greengrass V2
- Resource types defined by Amazon IoT Greengrass V2
- Condition keys for Amazon IoT Greengrass V2

Actions defined by Amazon IoT Greengrass 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 Amazon. 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.

> **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
AssociateServiceRoleToAccount	Grants permission to associate a role with your account. Amazon IoT Greengrass uses this role to access your Lambda functions and Amazon IoT resources	Permissions management			iam:PassRole
BatchAssociateClientDeviceWithCoreDevice	Grants permission to associate a list of client devices with a core device	Write	coreDevice*		
BatchDisassociateClientDevi	Grants permission to disassociate a list of client devices from a core device	Write	coreDevice*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ceFromCoreDevice					
CancelDeployment	Grants permission to cancel a deployment	Write	deployment*		iot:CancelJob iot:DeleteThingShadow iot:DescribeJob iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow iot:UpdateJob iot:UpdateThingShadow
CreateComponentVersion	Grants permission to create a component	Write	component*		

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
CreateDeployment	Grants permission to create a deployment	Write		aws:RequestTag/${TagKey} aws:TagKeys	iot:CancelJob iot:CreateJob iot:DeleteThingShadow iot:DescribeJob iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow iot:UpdateJob iot:UpdateThingShadow
DeleteComponent	Grants permission to delete a component	Write	componentVersion*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteCoreDevice	Grants permission to delete a Amazon IoT Greengrass core device, which is an Amazon IoT thing. This operation removes the core device from the list of core devices. This operation doesn't delete the Amazon IoT thing	Write	coreDevice*		iot:DescribeJobExecution
DeleteDeployment	Grants permission to delete a deployment. To delete an active deployment, it needs to be cancelled first	Write	deployment*		iot:DeleteJob
DescribeComponent	Grants permission to retrieve metadata for a version of a component	Read	componentVersion*		
DisassociateServiceRoleFromAccount	Grants permission to disassociate the service role from an account. Without a service role, deployments will not work	Write			
GetComponent	Grants permission to get the recipe for a version of a component	Read	componentVersion*		
GetComponentVersionArtifact	Grants permission to get the pre-signed URL to download a public component artifact	Read	componentVersion*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetConnectivityInfo	Grants permission to retrieve the connectivity information for a Greengrass core device	Read	connectivityInfo*		iot:GetThingShadow
GetCoreDevice	Grants permission to retrieves metadata for a Amazon IoT Greengrass core device	Read	coreDevice*		
GetDeployment	Grants permission to get a deployment	Read	deployment*		iot:DescribeJob iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow
GetServiceRoleForAccount	Grants permission to retrieve the service role that is attached to an account	Read			
ListClientDevicesAssociatedWithCoreDevice	Grants permission to retrieve a paginated list of client devices associated to a Amazon IoT Greengrass core device	List	coreDevice*		
ListComponentVersions	Grants permission to retrieve a paginated list of all versions for a component	List	component*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListComponents	Grants permission to retrieve a paginated list of component summaries	List			
ListCoreDevices	Grants permission to retrieve a paginated list of Amazon IoT Greengrass core devices	List			
ListDeployments	Grants permission to retrieves a paginated list of deployments	List			iot:DescribeJob iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListEffectiveDeployments	Grants permission to retrieves a paginated list of deployment jobs that Amazon IoT Greengrass sends to Amazon IoT Greengrass core devices	List	coreDevice*		iot:DescribeJob iot:DescribeJobExecution iot:DescribeThing iot:DescribeThingGroup iot:GetThingShadow
ListInstalledComponents	Grants permission to retrieve a paginated list of the components that a Amazon IoT Greengrass core device runs	List	coreDevice*		
ListTagsForResource	Grants permission to list the tags for a resource	Read	component		
			componentVersion		
			coreDevice		
			deployment		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
ResolveComponentCandidates	Grants permission to list components that meet the component, version, and platform requirements of a deployment	List	componentVersion*		
TagResource	Grants permission to add tags to a resource	Tagging	component		
			componentVersion		
			coreDevice		
			deployment		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagResource	Grants permission to remove tags from a resource	Tagging	component		
			componentVersion		
			coreDevice		
			deployment		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateConnectivityInfo	Grants permission to update the connectivity information for a Greengrass core. Any devices that belong to the group that has this core will receive this information in order to find the location of the core and connect to it	Write	connectivityInfo*		iot:GetThingShadow iot:UpdateThingShadow

Resource types defined by Amazon IoT Greengrass 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
connectivityInfo	`arn:${Partition}:greengrass:${Region}:${Account}:/greengrass/things/${ThingName}/connectivityInfo`	
component	`arn:${Partition}:greengrass:${Region}:${Account}:components:${ComponentName}`	aws:ResourceTag/${TagKey}
componentVersion	`arn:${Partition}:greengrass:${Region}:${Account}:components:${ComponentName}:versions:${ComponentVersion}`	aws:ResourceTag/${TagKey}
coreDevice	`arn:${Partition}:greengrass:${Region}:${Account}:coreDevices:${CoreDeviceThingName}`	aws:ResourceTag/${TagKey}
deployment	`arn:${Partition}:greengrass:${Region}:${Account}:deployments:${DeploymentId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon IoT Greengrass V2

Amazon IoT Greengrass 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 Amazon global condition context keys.

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

Actions, resources, and condition keys for Amazon IoT Jobs DataPlane

Amazon IoT Jobs DataPlane (service prefix: `iotjobsdata`) 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 IoT Jobs DataPlane
- Resource types defined by Amazon IoT Jobs DataPlane
- Condition keys for Amazon IoT Jobs DataPlane

Actions defined by Amazon IoT Jobs DataPlane

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 Amazon. 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.

> **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
DescribeJobExecution	Grants permission to describe a job execution	Read	thing*		
				iot:JobId	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetPendingJobExecutions	Grants permission to get the list of all jobs for a thing that are not in a terminal state	Read	thing*		
StartNextPendingJobExecution	Grants permission to get and start the next pending job execution for a thing	Write	thing*		
UpdateJobExecution	Grants permission to update a job execution	Write	thing*		
				iot:JobId	

Resource types defined by Amazon IoT Jobs DataPlane

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
thing	`arn:${Partition}:iot:${Region}:${Account}:thing/${ThingName}`	

Condition keys for Amazon IoT Jobs DataPlane

Amazon IoT Jobs DataPlane 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 Amazon global condition context keys.

Condition keys	Description	Type
iot:JobId	Filters access by jobId for iotjobsdata:DescribeJobExecution and iotjobsdata:UpdateJobExecution APIs	String

Actions, resources, and condition keys for Amazon IoT SiteWise

Amazon IoT SiteWise (service prefix: `iotsitewise`) 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 IoT SiteWise
- Resource types defined by Amazon IoT SiteWise
- Condition keys for Amazon IoT SiteWise

Actions defined by Amazon IoT SiteWise

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 Amazon. 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.

> **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 Assets	Grants permission to associate a child asset with a parent asset through a hierarchy	Write	asset*		
Associate TimeSerie	Grants permission to associate a time series with an asset property	Write	asset*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
sToAssetProperty			time-series*		
BatchAssociateProjectAssets	Grants permission to associate assets to a project	Write	project*		
BatchDisassociateProjectAssets	Grants permission to disassociate assets from a project	Write	project*		
BatchGetAssetPropertyAggregates	Grants permission to retrieve computed aggregates for multiple asset properties	Read	asset		
			time-series		
BatchGetAssetPropertyValue	Grants permission to retrieve the latest value for multiple asset properties	Read	asset		
			time-series		
BatchGetAssetPropertyValueHistory	Grants permission to retrieve the value history for multiple asset properties	Read	asset		
			time-series		
BatchPutAssetPropertyValue	Grants permission to put property values for asset properties	Write	asset		
			time-series		
CreateAccessPolicy	Grants permission to create an access policy for a portal or a project	Write	portal		
			project		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAsset	Grants permission to create an asset from an asset model	Write	asset-model*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAssetModel	Grants permission to create an asset model	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAssetModelCompositeModel	Grants permission to create an asset model composite model inside an asset model	Write	asset-model*		
CreateBulkImportJob	Grants permission to create bulk import job	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDashboard	Grants permission to create a dashboard in a project	Write	project*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataset	Grants permission to create a dataset	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateGateway	Grants permission to create a gateway	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePortal	Grants permission to create a portal	Write		aws:RequestTag/${TagKey} aws:TagKeys	sso:CreateManagedApplicationInstance sso:DescribeRegisteredRegions
CreateProject	Grants permission to create a project in a portal	Write	portal*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccessPolicy	Grants permission to delete an access policy	Write	access-policy*		
DeleteAsset	Grants permission to delete an asset	Write	asset*		
DeleteAssetModel	Grants permission to delete an asset model	Write	asset-model*		
DeleteAssetModelCompositeModel	Grants permission to delete an asset model composite model	Write	asset-model*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteDashboard	Grants permission to delete a dashboard	Write	dashboard*		
DeleteDataset	Grants permission to delete a dataset	Write	dataset*		
DeleteGateway	Grants permission to delete a gateway	Write	gateway*		
DeletePortal	Grants permission to delete a portal	Write	portal*		sso:DeleteManagedApplicationInstance
DeleteProject	Grants permission to delete a project	Write	project*		
DeleteTimeSeries	Grants permission to delete a time series	Write	asset		
			time-series		
DescribeAccessPolicy	Grants permission to describe an access policy	Read	access-policy*		
DescribeAction	Grants permission to describe actions	Read	asset		
DescribeAsset	Grants permission to describe an asset	Read	asset*		
DescribeAssetCompositeModel	Grants permission to describe an asset composite model	Read	asset*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeAssetModel	Grants permission to describe an asset model	Read	asset-model*		
DescribeAssetModelCompositeModel	Grants permission to describe an asset model composite model	Read	asset-model*		
DescribeAssetProperty	Grants permission to describe an asset property	Read	asset*		
DescribeBulkImportJob	Grants permission to describe bulk import job	Read			
DescribeDashboard	Grants permission to describe a dashboard	Read	dashboard*		
DescribeDataset	Grants permission to describe dataset	Read	dataset*		
DescribeDefaultEncryptionConfiguration	Grants permission to describe the default encryption configuration for the Amazon Web Services account	Read			
DescribeGateway	Grants permission to describe a gateway	Read	gateway*		
DescribeGatewayCapabilityConfiguration	Grants permission to describe a capability configuration for a gateway	Read	gateway*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeLoggingOptions	Grants permission to describe logging options for the Amazon Web Services account	Read			
DescribePortal	Grants permission to describe a portal	Read	portal*		
DescribeProject	Grants permission to describe a project	Read	project*		
DescribeStorageConfiguration	Grants permission to describe the storage configuration for the Amazon Web Services account	Read			
DescribeTimeSeries	Grants permission to describe a time series	Read	asset		
			time-series		
				aws:RequestTag/${TagKey} aws:TagKeys	
DisassociateAssets	Grants permission to disassociate a child asset from a parent asset by a hierarchy	Write	asset*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateTimeSeriesFromAssetProperty	Grants permission to disassociate a time series from an asset property	Write	asset*		
			time-series*		
EnableSiteWiseIntegration [permission only]	Grants permission to allow IoT SiteWise integrate with other services	Write			
ExecuteAction	Grants permission to execute actions	Write	asset		
ExecuteQuery	Grants permission to execute query	Read			
GetAssetPropertyAggregates	Grants permission to retrieve computed aggregates for an asset property	Read	asset		
			time-series		
GetAssetPropertyValue	Grants permission to retrieve the latest value for an asset property	Read	asset		
			time-series		
GetAssetPropertyValueHistory	Grants permission to retrieve the value history for an asset property	Read	asset		
			time-series		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetInterpolatedAssetPropertyValues	Grants permission to retrieve interpolated values for an asset property	Read	asset		
			time-series		
InvokeAssistant	Grants permission to invoke an assistant	Read			
ListAccessPolicies	Grants permission to list all access policies for an identity or a resource	List	portal		
			project		
ListActions	Grants permission to list all actions	List	asset		
ListAssetModelCompositeModels	Grants permission to list all asset model composite models	List	asset-model*		
ListAssetModelProperties	Grants permission to list asset model properties	List	asset-model*		
ListAssetModels	Grants permission to list all asset models	List			
ListAssetProperties	Grants permission to list asset properties	List	asset*		
ListAssetRelationships	Grants permission to list the asset relationship graph for an asset	List	asset*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAssets	Grants permission to list all assets	List	asset-model		
ListAssociatedAssets	Grants permission to list all assets associated with an asset through a hierarchy	List	asset*		
ListBulkImportJobs	Grants permission to list bulk import jobs	List			
ListCompositionRelationships	Grants permission to list all asset model composition relationships	List	asset-model*		
ListDashboards	Grants permission to list all dashboards in a project	List	project*		
ListDatasets	Grants permission to list all datasets	List			
ListGateways	Grants permission to list all gateways	List			
ListPortals	Grants permission to list all portals	List			
ListProjectAssets	Grants permission to list all assets associated with a project	List	project*		
ListProjects	Grants permission to list all projects in a portal	List	portal*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to list all tags for a resource	Read	access-policy		
			asset		
			asset-model		
			dashboard		
			dataset		
			gateway		
			portal		
			project		
			time-series		
				aws:ResourceTag/${TagKey}	
ListTimeSeries	Grants permission to list time series	List	asset		
PutDefaultEncryptionConfiguration	Grants permission to set the default encryption configuration for the Amazon Web Services account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutLoggingOptions	Grants permission to set logging options for the Amazon Web Services account	Write			
PutStorageConfiguration	Grants permission to configure storage settings for the Amazon Web Services account	Write			
TagResource	Grants permission to tag a resource	Tagging	access-policy		
			asset		
			asset-model		
			dashboard		
			dataset		
			gateway		
			portal		
			project		
			time-series		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to untag a resource	Tagging	access-policy		
			asset		
			asset-model		
			dashboard		
			dataset		
			gateway		
			portal		
			project		
			time-series		
				aws:TagKeys	
UpdateAccessPolicy	Grants permission to update an access policy	Write	access-policy*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAsset	Grants permission to update an asset	Write	asset*		
UpdateAssetModel	Grants permission to update an asset model	Write	asset-model*		
UpdateAssetModelCompositeModel	Grants permission to update asset model composite model	Write	asset-model*		
UpdateAssetModelPropertyRouting [permission only]	Grants permission to update an AssetModel property routing	Write	asset-model*		
UpdateAssetProperty	Grants permission to update an asset property	Write	asset*		
UpdateDashboard	Grants permission to update a dashboard	Write	dashboard*		
UpdateDataset	Grants permission to update a dataset	Write	dataset*		
UpdateGateway	Grants permission to update a gateway	Write	gateway*		
UpdateGatewayCapabilityConfiguration	Grants permission to update a capability configuration for a gateway	Write	gateway*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdatePortal	Grants permission to update a portal	Write	portal*		
UpdateProject	Grants permission to update a project	Write	project*		

Resource types defined by Amazon IoT SiteWise

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
asset	`arn:${Partition}:iotsitewise:${Region}:${Account}:asset/${AssetId}`	aws:ResourceTag/${TagKey}
asset-model	`arn:${Partition}:iotsitewise:${Region}:${Account}:asset-model/${AssetModelId}`	aws:ResourceTag/${TagKey}
time-series	`arn:${Partition}:iotsitewise:${Region}:${Account}:time-series/${TimeSeriesId}`	aws:ResourceTag/${TagKey}
gateway	`arn:${Partition}:iotsitewise:${Region}:${Account}:gateway/${GatewayId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
portal	`arn:${Partition}:iotsitewise:${Region}:${Account}:portal/${PortalId}`	aws:ResourceTag/${TagKey}
project	`arn:${Partition}:iotsitewise:${Region}:${Account}:project/${ProjectId}`	aws:ResourceTag/${TagKey}
dashboard	`arn:${Partition}:iotsitewise:${Region}:${Account}:dashboard/${DashboardId}`	aws:ResourceTag/${TagKey}
access-policy	`arn:${Partition}:iotsitewise:${Region}:${Account}:access-policy/${AccessPolicyId}`	aws:ResourceTag/${TagKey}
dataset	`arn:${Partition}:iotsitewise:${Region}:${Account}:dataset/${DatasetId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon IoT SiteWise

Amazon IoT SiteWise 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 Amazon 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

Condition keys	Description	Type
aws:TagKeys	Filters access by the tag keys in the request	ArrayOfString
iotsitewise:assetHierarchyPath	Filters access by an asset hierarchy path, which is the string of asset IDs in the asset's hierarchy, each separated by a forward slash	String
iotsitewise:childAssetId	Filters access by the ID of a child asset being associated whith a parent asset	String
iotsitewise:group	Filters access by the ID of an Amazon Single Sign-On group	String
iotsitewise:iam	Filters access by the ID of an Amazon IAM identity	String
iotsitewise:isAssociatedWithAssetProperty	Filters access by data streams associated with or not associated with asset properties	String
iotsitewise:portal	Filters access by the ID of a portal	String
iotsitewise:project	Filters access by the ID of a project	String
iotsitewise:propertyAlias	Filters access by the property alias	String
iotsitewise:propertyId	Filters access by the ID of an asset property	String
iotsitewise:user	Filters access by the ID of an Amazon Single Sign-On user	String

Actions, resources, and condition keys for Amazon IoT TwinMaker

Amazon IoT TwinMaker (service prefix: `iottwinmaker`) 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 IoT TwinMaker
- Resource types defined by Amazon IoT TwinMaker
- Condition keys for Amazon IoT TwinMaker

Actions defined by Amazon IoT TwinMaker

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 Amazon. 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.

> **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
BatchPutPropertyValues	Grants permission to set values for multiple time series properties	Write	workspace*		iottwinmaker:GetComponentType iottwinmaker:GetEntity iottwinmaker:GetWorkspace
			entity		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelMetadataTransferJob	Grants permission to cancel a metadata transfer job	Write	metadataTransferJob*		
CreateComponentType	Grants permission to create a componentType	Write	workspace*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateEntity	Grants permission to create an entity	Write	workspace*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateMetadataTransferJob	Grants permission to create a metadata transfer job	Write			
CreateScene	Grants permission to create a scene	Write	workspace*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSyncJob	Grants permission to create a sync job	Write	workspace*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkspace	Grants permission to create a workspace	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteComponentType	Grants permission to delete a componentType	Write	componentType*		
			workspace*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteEntity	Grants permission to delete an entity	Write	entity*		
			workspace*		
DeleteScene	Grants permission to delete a scene	Write	scene*		
			workspace*		
DeleteSyncJob	Grants permission to delete a sync job	Write	syncJob*		
			workspace*		
DeleteWorkspace	Grants permission to delete a workspace	Write	workspace*		
ExecuteQuery	Grants permission to execute query	Read	workspace*		
GetComponentType	Grants permission to get a componentType	Read	componentType*		
			workspace*		
GetEntity	Grants permission to get an entity	Read	entity*		
			workspace*		
GetMetadataTransferJob	Grants permission to get a metadata transfer job	Read	metadataTransferJob*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetPricingPlan	Grants permission to get pricing plan	Read			
GetPropertyValue	Grants permission to retrieve the property values	Read	workspace*		iottwinmaker:GetComponentType iottwinmaker:GetEntity iottwinmaker:GetWorkspace
			componentType		
			entity		
GetPropertyValueHistory	Grants permission to retrieve the time series value history	Read	workspace*		iottwinmaker:GetComponentType iottwinmaker:GetEntity iottwinmaker:GetWorkspace

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			componentType		
			entity		
GetScene	Grants permission to get a scene	Read	scene*		
			workspace*		
GetSyncJob	Grants permission to get a sync job	Read	syncJob*		
			workspace*		
GetWorkspace	Grants permission to get a workspace	Read	workspace*		
ListComponentTypes	Grants permission to list all componentTypes in a workspace	List	workspace*		
ListComponents	Grants permission to list components attached to an entity	List	entity*		
			workspace*		
ListEntities	Grants permission to list all entities in a workspace	List	workspace*		
ListMetadataTransferJobs	Grants permission to list all metadata transfer jobs	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListProperties	Grants permission to list properties of an entity component	List	entity*		
			workspace*		
ListScenes	Grants permission to list all scenes in a workspace	List	workspace*		
ListSyncJobs	Grants permission to list all sync jobs in a workspace	List	workspace*		
ListSyncResources	Grants permission to list all sync resources for a sync job	List	syncJob*		
			workspace*		
ListTagsForResource	Grants permission to list all tags for a resource	List	componentType		
			entity		
			scene		
			syncJob		
			workspace		
				aws:ResourceTag/${TagKey}	
ListWorkspaces	Grants permission to list all workspaces	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to tag a resource	Tagging	componentType		
			entity		
			scene		
			syncJob		
			workspace		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a resource	Tagging	componentType		
			entity		
			scene		
			syncJob		
			workspace		
				aws:TagKeys	
UpdateComponentType	Grants permission to update a componentType	Write	componentType*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			workspace*		
UpdateEntity	Grants permission to update an entity	Write	entity*		
			workspace*		
UpdatePricingPlan	Grants permission to update pricing plan	Write			
UpdateScene	Grants permission to update a scene	Write	scene*		
			workspace*		
UpdateWorkspace	Grants permission to update a workspace	Write	workspace*		

Resource types defined by Amazon IoT TwinMaker

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
workspace	`arn:${Partition}:iottwinmaker:${Region}:${Account}:workspace/${WorkspaceId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
entity	`arn:${Partition}:iottwinmaker:${Region}:${Account}:workspace/${WorkspaceId}/entity/${EntityId}`	aws:ResourceTag/${TagKey}
componentType	`arn:${Partition}:iottwinmaker:${Region}:${Account}:workspace/${WorkspaceId}/component-type/${ComponentTypeId}`	aws:ResourceTag/${TagKey}
scene	`arn:${Partition}:iottwinmaker:${Region}:${Account}:workspace/${WorkspaceId}/scene/${SceneId}`	aws:ResourceTag/${TagKey}
syncJob	`arn:${Partition}:iottwinmaker:${Region}:${Account}:workspace/${WorkspaceId}/sync-job/${SyncJobId}`	aws:ResourceTag/${TagKey}
metadataTransferJob	`arn:${Partition}:iottwinmaker:${Region}:${Account}:metadata-transfer-job/${MetadataTransferJobId}`	

Condition keys for Amazon IoT TwinMaker

Amazon IoT TwinMaker 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 Amazon 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 the request	ArrayOfString
iottwinmaker:destinationType	Filters access by destination type of metadata transfer job	ArrayOfString
iottwinmaker:linkedServices	Filters access by workspace linked to services	ArrayOfString
iottwinmaker:sourceType	Filters access by source type of metadata transfer job	ArrayOfString

Actions, resources, and condition keys for Amazon Key Management Service

Amazon 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 Amazon Key Management Service

- Resource types defined by Amazon Key Management Service
- Condition keys for Amazon Key Management Service

Actions defined by Amazon 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 Amazon. 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.

> **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 Amazon KMS key	Write	key*		
				kms:CallerAccount kms:ViaService	
ConnectCustomKeyStore	Controls permission to connect or reconnect a custom key store to its associated Amazon CloudHSM cluster or external key manager outside of Amazon	Write		kms:CallerAccount	
CreateAlias	Controls permission to create an alias for an Amazon 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 Amazon CloudHSM cluster or an external key manager outside of Amazon	Write		kms:CallerAccount	cloudhsm:DescribeClusters iam:CreateServiceLinkedRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateGrant	Controls permission to add a grant to an Amazon 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 Amazon 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 Amazon KMS key	Write	key*		
				kms:CallerAccount kms:EncryptionAlgorithm kms:EncryptionContext:${EncryptionContextKey} kms:EncryptionContextKeys kms:RecipientAttestation:ImageSha384 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	
DeleteAlias	Controls permission to delete an alias. Aliases are optional friendly names that you can associate with Amazon KMS keys	Write	alias*		
			key*		
				kms:CallerAccount kms:ViaService	
DeleteCustomKeyStore	Controls permission to delete a custom key store	Write		kms:CallerAccount	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteImportedKeyMaterial	Controls permission to delete cryptographic material that you imported into an Amazon KMS key. This action makes the key unusable	Write	key*		
				kms:CallerAccount kms:ViaService	
DeriveSharedSecret	Controls permission to use the specified Amazon 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:PCR0 kms:RecipientAttestation:PCR1 kms:RecipientAttestation:PCR2 kms:RecipientAttestation:PCR3 kms:RecipientAttes	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tation:PCR4 kms:RecipientAttestation:PCR5 kms:RecipientAttestation:PCR6 kms:RecipientAttestation:PCR7 kms:RecipientAttestation:PCR8 kms:RecipientAttestation:PCR9 kms:RecipientAttestation:PCR10	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR11 kms:RecipientAttestation:PCR12 kms:RecipientAttestation:PCR13 kms:RecipientAttestation:PCR14 kms:RecipientAttestation:PCR15 kms:RecipientAttestation:PCR16 kms:RecipientAttestation:PCR17	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR18 kms:RecipientAttestation:PCR19 kms:RecipientAttestation:PCR20 kms:RecipientAttestation:PCR21 kms:RecipientAttestation:PCR22 kms:RecipientAttestation:PCR23 kms:RecipientAttestation:PCR24	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR25 kms:RecipientAttestation:PCR26 kms:RecipientAttestation:PCR27 kms:RecipientAttestation:PCR28 kms:RecipientAttestation:PCR29 kms:RecipientAttestation:PCR30 kms:RecipientAttestation:PCR31	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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 Amazon KMS key	Read	key*		
				kms:CallerAccount kms:RequestAlias kms:ViaService	
DisableKey	Controls permission to disable an Amazon KMS key, which prevents it from being used in cryptographic operations	Write	key*		
				kms:CallerAccount kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisableKeyRotation	Controls permission to disable automatic rotation of a customer managed Amazon KMS key	Write	key*		
				kms:CallerAccount kms:ViaService	
DisconnectCustomKeyStore	Controls permission to disconnect the custom key store from its associated Amazon CloudHSM cluster or external key manager outside of Amazon	Write		kms:CallerAccount	
EnableKey	Controls permission to change the state of an Amazon KMS key to enabled. This allows the KMS key to be used in cryptographic operations	Write	key*		
				kms:CallerAccount kms:ViaService	
EnableKeyRotation	Controls permission to enable automatic rotation of the cryptographic material in an Amazon KMS key	Write	key*		
				kms:CallerAccount kms:RotationPeriodInDays kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Encrypt	Controls permission to use the specified Amazon KMS key to encrypt data and data keys	Write	key*		
				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 Amazon KMS key to generate data keys. You can use the data keys to encrypt data outside of Amazon KMS	Write	key*		
				kms:CallerAccount kms:EncryptionAlgorithm kms:EncryptionContext:${EncryptionContextKey} kms:EncryptionContextKeys kms:RecipientAttestation:ImageSha384 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	
GenerateDataKeyPair	Controls permission to use the Amazon 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:PCR0 kms:RecipientAttes	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tation:PCR1 kms:RecipientAttestation:PCR2 kms:RecipientAttestation:PCR3 kms:RecipientAttestation:PCR4 kms:RecipientAttestation:PCR5 kms:RecipientAttestation:PCR6 kms:RecipientAttestation:PCR7	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR8 kms:RecipientAttestation:PCR9 kms:RecipientAttestation:PCR10 kms:RecipientAttestation:PCR11 kms:RecipientAttestation:PCR12 kms:RecipientAttestation:PCR13 kms:RecipientAttestation:PCR14	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR15 kms:RecipientAttestation:PCR16 kms:RecipientAttestation:PCR17 kms:RecipientAttestation:PCR18 kms:RecipientAttestation:PCR19 kms:RecipientAttestation:PCR20 kms:RecipientAttestation:PCR21	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR22 kms:RecipientAttestation:PCR23 kms:RecipientAttestation:PCR24 kms:RecipientAttestation:PCR25 kms:RecipientAttestation:PCR26 kms:RecipientAttestation:PCR27 kms:RecipientAttestation:PCR28	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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 Amazon 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 Amazon 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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GenerateMac	Controls permission to use the Amazon KMS key to generate message authentication codes	Write	key*		
				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 Amazon KMS	Write		kms:RecipientAttestation:ImageSha384 kms:RecipientAttestation:PCR0 kms:RecipientAttestation:PCR1 kms:RecipientAttestation:PCR2 kms:RecipientAttestation:PCR3 kms:RecipientAttestation:PCR4 kms:RecipientAttes	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				tation:PCR5 kms:RecipientAttestation:PCR6 kms:RecipientAttestation:PCR7 kms:RecipientAttestation:PCR8 kms:RecipientAttestation:PCR9 kms:RecipientAttestation:PCR10 kms:RecipientAttestation:PCR11	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR12 kms:RecipientAttestation:PCR13 kms:RecipientAttestation:PCR14 kms:RecipientAttestation:PCR15 kms:RecipientAttestation:PCR16 kms:RecipientAttestation:PCR17 kms:RecipientAttestation:PCR18	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR19 kms:RecipientAttestation:PCR20 kms:RecipientAttestation:PCR21 kms:RecipientAttestation:PCR22 kms:RecipientAttestation:PCR23 kms:RecipientAttestation:PCR24 kms:RecipientAttestation:PCR25	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:RecipientAttestation:PCR26 kms:RecipientAttestation:PCR27 kms:RecipientAttestation:PCR28 kms:RecipientAttestation:PCR29 kms:RecipientAttestation:PCR30 kms:RecipientAttestation:PCR31	
GetKeyPolicy	Controls permission to view the key policy for the specified Amazon KMS key	Read	key*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:CallerAccount kms:ViaService	
GetKeyRotationStatus	Controls permission to view the key rotation status for an Amazon KMS key	Read	key*		
				kms:CallerAccount kms:ViaService	
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 Amazon KMS key	Read	key*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:CallerAccount kms:RequestAlias kms:ViaService	
ImportKeyMaterial	Controls permission to import cryptographic material into an Amazon KMS key	Write	key*		
				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 Amazon KMS keys	List			
ListGrants	Controls permission to view all grants for an Amazon KMS key	List	key*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				kms:CallerAccount kms:GrantIsForAWSResource kms:ViaService	
ListKeyPolicies	Controls permission to view the names of key policies for an Amazon KMS key	List	key*		
				kms:CallerAccount kms:ViaService	
ListKeyRotations	Controls permission to view the list of completed key rotations for an Amazon KMS key	List	key*		
				kms:CallerAccount kms:ViaService	
ListKeys	Controls permission to view the key ID and Amazon Resource Name (ARN) of all Amazon KMS keys in the account	List			
ListResourceTags	Controls permission to view all tags that are attached to an Amazon KMS key	List	key*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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			
PutKeyPolicy	Controls permission to replace the key policy for the specified Amazon 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 Amazon 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 Amazon 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 Amazon KMS key	Write	key*		
				kms:CallerAccount kms:ViaService	
ScheduleKeyDeletion	Controls permission to schedule deletion of an Amazon 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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Controls permission to create or update tags that are attached to an Amazon KMS key	Tagging	key*		
				aws:RequestTag/${TagKey} aws:TagKeys kms:CallerAccount kms:ViaService	
UntagResource	Controls permission to delete tags that are attached to an Amazon KMS key	Tagging	key*		
				aws:TagKeys kms:CallerAccount kms:ViaService	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAlias	Controls permission to associate an alias with a different Amazon KMS key. An alias is an optional friendly name that you can associate with a KMS key	Write	alias*		
			key*		
				kms:CallerAccount kms:ViaService	
UpdateCustomKeyStore	Controls permission to change the properties of a custom key store	Write		kms:CallerAccount	
UpdateKeyDescription	Controls permission to delete or change the description of an Amazon 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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Verify	Controls permission to use the specified Amazon KMS key to verify digital signatures	Write	key*		
				kms:CallerAccount kms:MessageType kms:RequestAlias kms:SigningAlgorithm kms:ViaService	
VerifyMac	Controls permission to use the Amazon KMS key to verify message authentication codes	Write	key*		
				kms:CallerAccount kms:MacAlgorithm kms:RequestAlias kms:ViaService	

Resource types defined by Amazon 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 Amazon Key Management Service

Amazon 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 Amazon global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access to the specified Amazon KMS operations based on both the key and value of the tag in the request	String
aws:ResourceTag/${TagKey}	Filters access to the specified Amazon KMS operations based on tags assigned to the Amazon KMS key	String
aws:TagKeys	Filters access to the specified Amazon 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 Amazon KMS operations based on the Amazon Web Services account ID of the caller. You can use this condition key to allow or deny access to all IAM users and roles in an Amazon Web Services 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 Amazon 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 Amazon 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 Amazon 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 Amazon 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 Amazon 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 Amazon 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 Amazon 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 Amazon 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 Amazon 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:PCR0	Filters access by the platform configuration register (PCR) 0 in the attestation document. PCR0 is a contiguous measure of the contents of the enclave image file, without the section data	String
kms:RecipientAttestation:PCR1	Filters access by the platform configuration register (PCR) 1 in the attestation document. 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

Condition keys	Description	Type
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
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

Condition keys	Description	Type
kms:RecipientAttestation:PCR2	Filters access by the platform configuration register (PCR) 2 in the attestation document. 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
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

Condition keys	Description	Type
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
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. 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

Condition keys	Description	Type
kms:RecipientAttestation:PCR4	Filters access by the platform configuration register (PCR) 4 in the attestation document. 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
kms:RecipientAttestation:PCR7	Filters access by 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. 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

Condition keys	Description	Type
kms:ResourceAliases	Filters access to specified Amazon KMS operations based on aliases associated with the Amazon 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
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 Amazon 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 Analytics

Amazon Kinesis Analytics (service prefix: `kinesisanalytics`) 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 Analytics
- Resource types defined by Amazon Kinesis Analytics
- Condition keys for Amazon Kinesis Analytics

Actions defined by Amazon Kinesis Analytics

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 Amazon. 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.

> **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
AddApplicationInput	Grants permission to add input to the application	Write	application*		
AddApplicationOutput	Grants permission to add output to the application	Write	application*		
AddApplicationReferenceDataSource	Grants permission to add reference data source to the application	Write	application*		
CreateApplication	Grants permission to create an application	Write		aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
DeleteApplication	Grants permission to delete the application	Write	application*		
DeleteApplicationOutput	Grants permission to delete the specified output of the application	Write	application*		
DeleteApplicationReferenceDataSource	Grants permission to delete the specified reference data source of the application	Write	application*		
DescribeApplication	Grants permission to describe the specified application	Read	application*		
DiscoverInputSchema	Grants permission to discover the input schema for the application	Read			
GetApplicationState [permission only]	Grants permission to Kinesis Data Analytics console to display stream results for Kinesis Data Analytics SQL runtime applications	Read	application*		
ListApplications	Grants permission to list applications for the account	List			
ListTagsForResource	Grants permission to fetch the tags associated with the application	Read	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartApplication	Grants permission to start the application	Write	application*		
StopApplication	Grants permission to stop the application	Write	application*		
TagResource	Grants permission to add tags to the application	Tagging	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove the specified tags from the application	Tagging	application*		
				aws:TagKeys	
UpdateApplication	Grants permission to update the application	Write	application*		

Resource types defined by Amazon Kinesis Analytics

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:${Partition}:kinesisanalytics:${Region}:${Account}:application/${ApplicationName}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Kinesis Analytics

Amazon Kinesis Analytics 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 Amazon global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by set of values for each of the tags	String
aws:ResourceTag/${TagKey}	Filters access by tag-value assoicated with the resource	String
aws:TagKeys	Filters access by the presence of mandatory tag keys in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Kinesis Analytics V2

Amazon Kinesis Analytics V2 (service prefix: `kinesisanalytics`) 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 Analytics V2
- Resource types defined by Amazon Kinesis Analytics V2
- Condition keys for Amazon Kinesis Analytics V2

Actions defined by Amazon Kinesis Analytics 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 Amazon. 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.

> **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
AddApplicationCloudWatchLoggingOption	Grants permission to add cloudwatch logging option to the application	Write	application*		
AddApplicationInput	Grants permission to add input to the application	Write	application*		
AddApplicationInputProcessingConfiguration	Grants permission to add input processing configuration to the application	Write	application*		
AddApplicationOutput	Grants permission to add output to the application	Write	application*		
AddApplicationReferenceDataSource	Grants permission to add reference data source to the application	Write	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddApplicationVpcConfiguration	Grants permission to add VPC configuration to the application	Write	application*		
CreateApplication	Grants permission to create an application	Write		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
CreateApplicationPresignedUrl	Grants permission to create and return a URL that you can use to connect to an application's extension	Read	application*		
CreateApplicationSnapshot	Grants permission to create a snapshot for an application	Write	application*		
DeleteApplication	Grants permission to delete the application	Write	application*		
DeleteApplicationCloudWatchLoggingOption	Grants permission to delete the specified cloudwatch logging option of the application	Write	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteApplicationInputProcessingConfiguration	Grants permission to delete the specified input processing configuration of the application	Write	application*		
DeleteApplicationOutput	Grants permission to delete the specified output of the application	Write	application*		
DeleteApplicationReferenceDataSource	Grants permission to delete the specified reference data source of the application	Write	application*		
DeleteApplicationSnapshot	Grants permission to delete a snapshot for an application	Write	application*		
DeleteApplicationVpcConfiguration	Grants permission to delete the specified VPC configuration of the application	Write	application*		
DescribeApplication	Grants permission to describe the specified application	Read	application*		
DescribeApplicationOperation	Grants permission to describe an application operation of an application	Read	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeApplicationSnapshot	Grants permission to describe an application snapshot	Read	application*		
DescribeApplicationVersion	Grants permission to describe the application version of an application	Read	application*		
DiscoverInputSchema	Grants permission to discover the input schema for the application	Read			iam:PassRole
ListApplicationOperations	Grants permission to list application operations of an application	Read	application*		
ListApplicationSnapshots	Grants permission to list the snapshots for an application	Read	application*		
ListApplicationVersions	Grants permission to list application versions of an application	Read	application*		
ListApplications	Grants permission to list applications for the account	List			
ListTagsForResource	Grants permission to fetch the tags associated with the application	Read	application*		
RollbackApplication	Grants permission to perform rollback operation on an application	Write	application*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartApplication	Grants permission to start the application	Write	application*		
StopApplication	Grants permission to stop the application	Write	application*		
TagResource	Grants permission to add tags to the application	Tagging	application*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove the specified tags from the application	Tagging	application*		
				aws:TagKeys	
UpdateApplication	Grants permission to update the application	Write	application*		
UpdateApplicationMaintenanceConfiguration	Grants permission to update the maintenance configuration of an application	Write	application*		

Resource types defined by Amazon Kinesis Analytics 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
application	`arn:${Partition}:kinesisanalytics:${Region}:${Account}:application/${ApplicationName}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Kinesis Analytics V2

Amazon Kinesis Analytics 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 Amazon global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by set of values for each of the tags	String
aws:ResourceTag/${TagKey}	Filters access by tag-value assoicated with the resource	String
aws:TagKeys	Filters access by the presence of mandatory tag keys in the request	ArrayOfString

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 Amazon. 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.

> **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	

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeregisterStreamConsumer	Grants permission to deregister a stream consumer with a Kinesis data stream	Write	consumer*	aws:ResourceTag/${TagKey}	
DescribeLimits	Grants permission to describe the shard limits and usage for the account	Read			
DescribeStream	Grants permission to describe the specified stream	Read	stream*	aws:ResourceTag/${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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRecords	Grants permission to get data records from a shard	Read	stream*	aws:ResourceTag/${TagKey}	
GetResourcePolicy	Grants permission to get a resource policy associated with a specified stream or consumer	Read	consumer*	aws:ResourceTag/${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/${TagKey}	
ListShards	Grants permission to list the shards in a stream and provides information about each shard	List	stream*	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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}	
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}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 Amazon 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}	
UpdateShardCount	Grants permission to update the shard count of the specified stream to the specified number of shards	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateStreamMode	Grants permission to update the capacity mode of the data stream	Write			

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/${TagKey}
consumer	`arn:${Partition}:kinesis:${Region}:${Account}:${StreamType}/${StreamName}/consumer/${ConsumerName}:${ConsumerCreationTimpstamp}`	
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 Amazon 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 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 Amazon. 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.

> **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*		
				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	Write	deliverystream*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	throughput per producer than when writing single records				
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 Amazon 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 Kinesis Video Streams

Amazon Kinesis Video Streams (service prefix: `kinesisvideo`) 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 Video Streams
- Resource types defined by Amazon Kinesis Video Streams
- Condition keys for Amazon Kinesis Video Streams

Actions defined by Amazon Kinesis Video 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 Amazon. 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.

> **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
ConnectAsMaster	Grants permission to connect as a master to the signaling channel specified by the endpoint	Write	channel*		
ConnectAsViewer	Grants permission to connect as a viewer to the signaling channel specified by the endpoint	Write	channel*		
CreateSignalingChannel	Grants permission to create a signaling channel	Write	channel*		
				aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
CreateStream	Grants permission to create a Kinesis video stream	Write	stream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteEdgeConfiguration	Grants permission to delete the edge configuration of your Kinesis Video Stream	Write	stream*		
DeleteSignalingChannel	Grants permission to delete an existing signaling channel	Write	channel*		
DeleteStream	Grants permission to delete an existing Kinesis video stream	Write	stream*		
DescribeEdgeConfiguration	Grants permission to describe the edge configuration of your Kinesis Video Stream	Read	stream*		
DescribeImageGenerationConfiguration	Grants permission to describe the image generation configuration of your Kinesis video stream	Read	stream*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeMappedResourceConfiguration	Grants permission to describe the resource mapped to the Kinesis video stream	List	stream*		
DescribeMediaStorageConfiguration	Grants permission to describe the media storage configuration of a signaling channel	Read	channel*		
DescribeNotificationConfiguration	Grants permission to describe the notification configuration of your Kinesis video stream	Read	stream*		
DescribeSignalingChannel	Grants permission to describe the specified signaling channel	List	channel*		
DescribeStream	Grants permission to describe the specified Kinesis video stream	List	stream*		
GetClip	Grants permission to get a media clip from a video stream	Read	stream*		
GetDASHStreamingSessionURL	Grants permission to create a URL for MPEG-DASH video streaming	Read	stream*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDataEndpoint	Grants permission to get an endpoint for a specified stream for either reading or writing media data to Kinesis Video Streams	Read	stream*		
GetHLSStreamingSessionURL	Grants permission to create a URL for HLS video streaming	Read	stream*		
GetIceServerConfig	Grants permission to get the ICE server configuration	Read	channel*		
GetImages	Grants permission to get generated images from your Kinesis video stream	Read	stream*		
GetMedia	Grants permission to return media content of a Kinesis video stream	Read	stream*		
GetMediaForFragmentList	Grants permission to read and return media data only from persisted storage	Read	stream*		
GetSignalingChannelEndpoint	Grants permission to get endpoints for a specified combination of protocol and role for a signaling channel	Read	channel*		
JoinStorageSession	Grants permission to join a storage session for a channel	Write	channel*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
JoinStorageSessionAsViewer	Grants permission to join a storage session for a channel as viewer	Write	channel*		
ListEdgeAgentConfigurations	Grants permission to list an edge agent configurations	List			
ListFragments	Grants permission to list the fragments from archival storage based on the pagination token or selector type with range specified	List	stream*		
ListSignalingChannels	Grants permission to list your signaling channels	List			
ListStreams	Grants permission to list your Kinesis video streams	List			
ListTagsForResource	Grants permission to fetch the tags associated with your resource	Read	channel		
			stream		
ListTagsForStream	Grants permission to fetch the tags associated with Kinesis video stream	Read	stream*		
PutMedia	Grants permission to send media data to a Kinesis video stream	Write	stream*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SendAlexaOfferToMaster	Grants permission to send the Alexa SDP offer to the master	Write	channel*		
StartEdgeConfigurationUpdate	Grants permission to start edge configuration update of your Kinesis Video Stream	Write	stream*		
TagResource	Grants permission to attach set of tags to your resource	Tagging	channel		
			stream		
				aws:RequestTag/${TagKey} aws:TagKeys	
TagStream	Grants permission to attach set of tags to your Kinesis video streams	Tagging	stream*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove one or more tags from your resource	Tagging	channel		
			stream		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
UntagStream	Grants permission to remove one or more tags from your Kinesis video streams	Tagging	stream*		
				aws:TagKeys	
UpdateDataRetention	Grants permission to update the data retention period of your Kinesis video stream	Write	stream*		
UpdateImageGenerationConfiguration	Grants permission to update the image generation configuration of your Kinesis video stream	Write	stream*		
UpdateMediaStorageConfiguration	Grants permission to create or update an mapping between a signaling channel and stream	Write	channel*		
UpdateNotificationConfiguration	Grants permission to update the notification configuration of your Kinesis video stream	Write	stream*		
UpdateSignalingChannel	Grants permission to update an existing signaling channel	Write	channel*		
UpdateStream	Grants permission to update an existing Kinesis video stream	Write	stream*		

Resource types defined by Amazon Kinesis Video 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:${Partition}:kinesisvideo:${Region}:${Account}:stream/${StreamName}/${CreationTime}`	aws:ResourceTag/${TagKey}
channel	`arn:${Partition}:kinesisvideo:${Region}:${Account}:channel/${ChannelName}/${CreationTime}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Kinesis Video Streams

Amazon Kinesis Video 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 Amazon global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters requests based on the allowed set of values for each of the tags	String
aws:ResourceTag/${TagKey}	Filters actions based on tag-value assoicated with the stream	String

Condition keys	Description	Type
aws:TagKeys	Filters requests based on the presence of mandatory tag keys in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Lambda

Amazon 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 Amazon Lambda
- Resource types defined by Amazon Lambda
- Condition keys for Amazon Lambda

Actions defined by Amazon 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 Amazon. 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.

> **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 Amazon Lambda layer	Permissions management	layerVersion*		
AddPermission	Grants permission to give an Amazon service or another account permission to use an Amazon Lambda function	Permissions management	function*		
				lambda:PrincipalOrgID	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				lambda:FunctionUrlAuthType	
CreateAlias	Grants permission to create an alias for a Lambda function version	Write	function*		
CreateCodeSigningConfig	Grants permission to create an Amazon Lambda code signing config	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateEventSourceMapping	Grants permission to create a mapping between an event source and an Amazon Lambda function	Write		lambda:FunctionArn aws:RequestTag/${TagKey} aws:TagKeys	
CreateFunction	Grants permission to create an Amazon Lambda function	Write	function*		iam:PassRole

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 Amazon Lambda function alias	Write	function*		
DeleteCodeSigningConfig	Grants permission to delete an Amazon Lambda code signing config	Write	code signing config*		
DeleteEventSourceMapping	Grants permission to delete an Amazon Lambda event source mapping	Write	eventSourceMapping*		
				lambda:FunctionArn	
DeleteFunction	Grants permission to delete an Amazon Lambda function	Write	function*		
DeleteFunctionCodeSigningConfig	Grants permission to detach a code signing config from an Amazon Lambda function	Write	function*		
DeleteFunctionConcurrency	Grants permission to remove a concurrent execution limit from an Amazon Lambda function	Write	function*		
DeleteFunctionEventInvokeConfig	Grants permission to delete the configuration for asynchronous invocation for an Amazon Lambda function, version, or alias	Write	function*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 Amazon Lambda layer	Write	layerVersion*		
DeleteProvisionedConcurrencyConfig	Grants permission to delete the provisioned concurrency configuration for an Amazon 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*		
GetAccountSettings	Grants permission to view details about an account's limits and usage in an Amazon Web Services Region	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAlias	Grants permission to view details about an Amazon Lambda function alias	Read	function*		
GetCodeSigningConfig	Grants permission to view details about an Amazon Lambda code signing config	Read	code signing config*		
GetEventSourceMapping	Grants permission to view details about an Amazon Lambda event source mapping	Read	eventSourceMapping*		
				lambda:FunctionArn	
GetFunction	Grants permission to view details about an Amazon Lambda function	Read	function*		
GetFunctionCodeSigningConfig	Grants permission to view the code signing config arn attached to an Amazon 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 Amazon Lambda function or version	Read	function*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 Amazon Lambda function	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 Amazon 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 Amazon Lambda layer	Read	layerVersion*		
GetPolicy	Grants permission to view the resource-based policy for an Amazon 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 Amazon Lambda function's alias or version	Read	function alias		
			function version		
GetRuntimeManagementConfig	Grants permission to view the runtime management configuration of an Amazon Lambda function	Read	function*		
InvokeAsync	Grants permission to invoke a function asynchronously (Deprecated)	Write	function*		
InvokeFunction	Grants permission to invoke an Amazon Lambda function	Write	function*		
				lambda:EventSourceToken	
InvokeFunctionUrl [permission only]	Grants permission to invoke an Amazon Lambda function through url	Write	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn lambda:EventSourceToken	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAliases	Grants permission to retrieve a list of aliases for an Amazon Lambda function	List	function*		
ListCodeSigningConfigs	Grants permission to retrieve a list of Amazon Lambda code signing configs	List			
ListEventSourceMappings	Grants permission to retrieve a list of Amazon Lambda event source mappings	List			
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	
ListFunctions	Grants permission to retrieve a list of Amazon Lambda functions, with the version-specific configuration of each function	List			
ListFunctionsByCodeSigningConfig	Grants permission to retrieve a list of Amazon Lambda functions by the code signing config assigned	List	code signing config*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListLayerVersions	Grants permission to retrieve a list of versions of an Amazon Lambda layer	List			
ListLayers	Grants permission to retrieve a list of Amazon 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 Amazon Lambda function	List	function*		
ListTags	Grants permission to retrieve a list of tags for an Amazon Lambda function, event source mapping or code signing configuration resource	Read	code signing config		
			eventSourceMapping		
			function		
ListVersionsByFunction	Grants permission to retrieve a list of versions for an Amazon Lambda function	List	function*		
PublishLayerVersion	Grants permission to create an Amazon Lambda layer	Write	layer*		
PublishVersion	Grants permission to create an Amazon Lambda function version	Write	function*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutFunctionCodeSigningConfig	Grants permission to attach a code signing config to an Amazon Lambda function	Write	code signing config*		
			function*		
				lambda:CodeSigningConfigArn	
PutFunctionConcurrency	Grants permission to configure reserved concurrency for an Amazon Lambda function	Write	function*		
PutFunctionEventInvokeConfig	Grants permission to configures options for asynchronous invocation on an Amazon Lambda function, version, or alias	Write	function*		
PutFunctionRecursionConfig	Grants permission to update the recursion configuration of an Amazon Lambda function	Write	function*		
PutProvisionedConcurrencyConfig	Grants permission to configure provisioned concurrency for an Amazon Lambda function's alias or version	Write	function alias		
			function version		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutRuntimeManagementConfig	Grants permission to update the runtime management configuration of an Amazon Lambda function	Write	function*		
RemoveLayerVersionPermission	Grants permission to remove a statement from the permissions policy for a version of an Amazon Lambda layer	Permissions management	layerVersion*		
RemovePermission	Grants permission to revoke function-use permission from an Amazon service or another account	Permissions management	function*		
				lambda:Principal lambda:FunctionUrlAuthType	
TagResource	Grants permission to add tags to an Amazon Lambda function, event source mapping or code signing configuration resource	Tagging	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 Amazon Lambda function, event source mapping or code signing configuration resource	Tagging	code signing config		
			eventSourceMapping		
			function		
				aws:TagKeys	
UpdateAlias	Grants permission to update the configuration of an Amazon Lambda function's alias	Write	function*		
UpdateCodeSigningConfig	Grants permission to update an Amazon Lambda code signing config	Write	code signing config*		
UpdateEventSourceMapping	Grants permission to update the configuration of an Amazon Lambda event source mapping	Write	eventSourceMapping*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				lambda:FunctionArn	
UpdateFunctionCode	Grants permission to update the code of an Amazon Lambda function	Write	function*		
UpdateFunctionCodeSigningConfig	Grants permission to update the code signing config of an Amazon Lambda function	Write	code signing config*		
			function*		
UpdateFunctionConfiguration	Grants permission to modify the version-specific settings of an Amazon Lambda function	Write	function*		
				lambda:Layer lambda:VpcIds lambda:SubnetIds lambda:SecurityGroupIds	
UpdateFunctionEventInvokeConfig	Grants permission to modify the configuration for asynchronous invocation for an Amazon Lambda function, version, or alias	Write	function*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateFunctionUrlConfig	Grants permission to update a function url configuration for a Lambda function	Write	function*		
				lambda:FunctionUrlAuthType lambda:FunctionArn	

Resource types defined by Amazon 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
code signing config	`arn:${Partition}:lambda:${Region}:${Account}:code-signing-config:${CodeSigningConfigId}`	aws:ResourceTag/${TagKey}
eventSourceMapping	`arn:${Partition}:lambda:${Region}:${Account}:event-source-mapping:${UUID}`	aws:ResourceTag/${TagKey}
function	`arn:${Partition}:lambda:${Region}:${Account}:function:${FunctionName}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
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 Amazon Lambda

Amazon 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 Amazon 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

Condition keys	Description	Type
lambda:CodeSigningConfigArn	Filters access by the ARN of an Amazon Lambda code signing config	ARN
lambda:EventSourceToken	Filters access by the ID from a non-Amazon event source configured for the Amazon Lambda function	String
lambda:FunctionArn	Filters access by the ARN of an Amazon 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
lambda:Layer	Filters access by the ARN of a version of an Amazon Lambda layer	ArrayOfString
lambda:Principal	Filters access by restricting the Amazon service or account that can invoke a function	String
lambda:SecurityGroupIds	Filters access by the ID of security groups configured for the Amazon Lambda function	ArrayOfString
lambda:SourceFunctionArn	Filters access by the ARN of the Amazon Lambda function from which the request originated	ARN
lambda:SubnetIds	Filters access by the ID of subnets configured for the Amazon Lambda function	ArrayOfString
lambda:VpcIds	Filters access by the ID of the VPC configured for the Amazon Lambda function	String

Actions, resources, and condition keys for Amazon Launch Wizard

Amazon Launch Wizard (service prefix: `launchwizard`) 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 Launch Wizard
- Resource types defined by Amazon Launch Wizard
- Condition keys for Amazon Launch Wizard

Actions defined by Amazon Launch Wizard

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 Amazon. 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.

> **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
CreateAdditionalNode [permission only]	Grants permission to create an additional node	Write			
CreateDeployment	Grants permission to create a deployment	Write	deployment*	aws:RequestTag/${TagKey} aws:TagKeys	
CreateSettingsSet	Grants permission to create an application settings set	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
[permission only]					
DeleteAdditionalNode [permission only]	Grants permission to delete an additional node	Write			
DeleteApp [permission only]	Grants permission to delete an application	Write			
DeleteDeployment	Grants permission to delete a deployment	Write	deployment*	aws:ResourceTag/${TagKey}	
DeleteSettingsSet [permission only]	Grants permission to delete a settings set	Write			
DescribeAdditionalNode [permission only]	Grants permission to describe an additional node	Read			
DescribeProvisionedApp [permission only]	Grants permission to describe provisioning applications	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeProvisioningEvents [permission only]	Grants permission to describe provisioning events	Read			
DescribeSettingsSet [permission only]	Grants permission to describe an application settings set	Read			
GetDeployment	Grants permission to get a deployment	Read	deployment*	aws:ResourceTag/${TagKey}	
GetInfrastructureSuggestion [permission only]	Grants permission to get infrastructure suggestion	Read			
GetIpAddress [permission only]	Grants permission to get customer's ip address	Read			
GetResourceCostEstimate [permission only]	Grants permission to get resource cost estimate	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetResourceRecommendation [permission only]	Grants permission to get recommendation for a resource	Read			
GetSettingsSet [permission only]	Grants permission to get a settings set	Read			
GetWorkload	Grants permission to get a workload	Read			
GetWorkloadAsset [permission only]	Grants permission to get a workload's asset	Read			
GetWorkloadAssets [permission only]	Grants permission to get workload assets	Read			
GetWorkloadDeploymentPattern	Grants permission to get a deployment pattern	Read			
ListAdditionalNodes [permission only]	Grants permission to list additional nodes	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAllowedResources [permission only]	Grants permission to list the allowed resources	List			
ListDeploymentEvents	Grants permission to list the events that occured during a deployment	List			
ListDeployments	Grants permission to list deployments	List			
ListProvisionedApps [permission only]	Grants permission to list provisioning applications	List			
ListResourceCostEstimates [permission only]	Grants permission to list the cost estimates of resources	List			
ListSettingsSets [permission only]	Grants permission to list settings sets	List			
ListTagsForResource	Grants permission to list tags for a LaunchWizard resource.	Read	deployment	aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListWorkloadDeploymentOptions [permission only]	Grants permission to list deployment options of a given workload	List			
ListWorkloadDeploymentPatterns	Grants permission to list the deployment patterns of a workload	List			
ListWorkloads	Grants permission to list workloads	List			
PutSettingsSet [permission only]	Grants permission to create a settings set	Write			
StartProvisioning [permission only]	Grants permission to start a provisioning	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to tag a LaunchWizard resource.	Tagging	deployment	aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to untag a LaunchWizard resource.	Tagging	deployment	aws:TagKeys	
UpdateSettingsSet [permission only]	Grants permission to update an application settings set	Write			

Resource types defined by Amazon Launch Wizard

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
deployment	`arn:${Partition}:launchwizard:${Region}:${Account}:deployment/${DeploymentId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Launch Wizard

Amazon Launch Wizard 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 Amazon global condition context keys.

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

Actions, resources, and condition keys for Amazon License Manager

Amazon License Manager (service prefix: `license-manager`) 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 License Manager
- Resource types defined by Amazon License Manager
- Condition keys for Amazon License Manager

Actions defined by Amazon License 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 Amazon. 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.

> **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
AcceptGrant	Grants permission to accept a grant	Write	grant*		
CheckInLicense	Grants permission to check in license entitlements back to pool	Write			
CheckoutBorrowLicense	Grants permission to check out license entitlements for borrow use case	Write	license*		
CheckoutLicense	Grants permission to check out license entitlements	Write			
CreateGrant	Grants permission to create a new grant for license	Write	license*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateGrantVersion	Grants permission to create new version of grant	Write	grant*		
CreateLicense	Grants permission to create a new license	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLicenseConfiguration	Grants permission to create a new license configuration	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLicenseConversionTaskForResource	Grants permission to create a license conversion task for a resource	Write			
CreateLicenseManagerReportGenerator	Grants permission to create a report generator for a license configuration	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLicenseVersion	Grants permission to create new version of license	Write	license*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateToken	Grants permission to create a new token for license	Write	license*		
DeleteGrant	Grants permission to delete a grant	Write	grant*		
DeleteLicense	Grants permission to delete a license	Write	license*		
DeleteLicenseConfiguration	Grants permission to permanently delete a license configuration	Write	license-configuration*		
DeleteLicenseManagerReportGenerator	Grants permission to delete a report generator	Write	report-generator*		
DeleteToken	Grants permission to delete token	Write			
ExtendLicenseConsumption	Grants permission to extend consumption period of already checkout license entitlements	Write			
GetAccessToken	Grants permission to get access token	Read			
GetGrant	Grants permission to get a grant	Read	grant*		
GetLicense	Grants permission to get a license	Read	license*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetLicenseConfiguration	Grants permission to get a license configuration	Read	license-configuration*		
GetLicenseConversionTask	Grants permission to retrieve a license conversion task	Read			
GetLicenseManagerReportGenerator	Grants permission to get a report generator	Read	report-generator*		
GetLicenseUsage	Grants permission to get a license usage	Read	license*		
GetServiceSettings	Grants permission to get service settings	List			
ListAssociationsForLicenseConfiguration	Grants permission to list associations for a selected license configuration	List	license-configuration*		
ListDistributedGrants	Grants permission to list distributed grants	List			
ListFailuresForLicenseConfigurationOperations	Grants permission to list the license configuration operations that failed	List	license-configuration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListLicenseConfigurations	Grants permission to list license configurations	Read			
ListLicenseConversionTasks	Grants permission to list license conversion tasks	List			
ListLicenseManagerReportGenerators	Grants permission to list report generators	List	license-configuration		
ListLicenseSpecificationsForResource	Grants permission to list license specifications associated with a selected resource	List			
ListLicenseVersions	Grants permission to list license versions	List	license*		
ListLicenses	Grants permission to list licenses	Read			
ListReceivedGrants	Grants permission to list received grants	List			
ListReceivedGrantsForOrganization	Grants permission to list received grants for organization	List			
ListReceivedLicenses	Grants permission to list received licenses	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListReceivedLicensesForOrganization	Grants permission to list received licenses for organization	List			
ListResourceInventory	Grants permission to list resource inventory	List			
ListTagsForResource	Grants permission to list tags for a selected resource	Read	grant		
			license		
			license-configuration		
			report-generator		
ListTokens	Grants permission to list tokens	List			
ListUsageForLicenseConfiguration	Grants permission to list usage records for selected license configuration	List	license-configuration*		
RejectGrant	Grants permission to reject a grant	Write	grant*		
TagResource	Grants permission to tag a selected resource	Tagging	grant		
			license		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			license-configuration		
			report-generator		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to untag a selected resource	Tagging	grant		
			license		
			license-configuration		
			report-generator		
				aws:TagKeys	
UpdateLicenseConfiguration	Grants permission to update an existing license configuration	Write	license-configuration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateLicenseManagerReportGenerator	Grants permission to update a report generator for a license configuration	Write	report-generator*		
UpdateLicenseSpecificationsForResource	Grants permission to updates license specifications for a selected resource	Write	license-configuration*		
UpdateServiceSettings	Grants permission to updates service settings	Permissions management			

Resource types defined by Amazon License 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
license-configuration	`arn:${Partition}:license-manager:${Region}:${Account}:license-configuration:${LicenseConfigurationId}`	aws:ResourceTag/${TagKey} license-manager:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
license	`arn:${Partition}:license-manager::${Account}:license:${LicenseId}`	aws:ResourceTag/${TagKey}
grant	`arn:${Partition}:license-manager::${Account}:grant:${GrantId}`	aws:ResourceTag/${TagKey}
report-generator	`arn:${Partition}:license-manager:${Region}:${Account}:report-generator:${ReportGeneratorId}`	aws:ResourceTag/${TagKey} license-manager:ResourceTag/${TagKey}

Condition keys for Amazon License Manager

Amazon License 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 Amazon 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 tag keys that are passed in the request	ArrayOfString
license-manager:Re	Filters access by the tag key-value pairs attached to the resource	String

Condition keys	Description	Type
sourceTag/${TagKey}		

Actions, resources, and condition keys for Amazon License Manager Linux Subscriptions Manager

Amazon License Manager Linux Subscriptions Manager (service prefix: `license-manager-linux-subscriptions`) 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 License Manager Linux Subscriptions Manager
- Resource types defined by Amazon License Manager Linux Subscriptions Manager
- Condition keys for Amazon License Manager Linux Subscriptions Manager

Actions defined by Amazon License Manager Linux Subscriptions 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 Amazon. 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.

> **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
DeregisterSubscriptionProvider	Grants permission to permanently delete a subscription provider in Amazon License Manager	Write	subscription-provider*		
GetRegisteredSubsc	Grants permission to get a subscription provider in Amazon License Manager	Read	subscription-provider*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
riptionProvider					
GetServiceSettings	Grants permission to get the service settings for Linux subscriptions in Amazon License Manager	Read			
ListLinuxSubscriptionInstances	Grants permission to list all instances with Linux subscriptions in Amazon License Manager	Read			
ListLinuxSubscriptions	Grants permission to list all Linux subscriptions in Amazon License Manager	Read			
ListRegisteredSubscriptionProviders	Grants permission to list subscription providers in Amazon License Manager	Read			
ListTagsForResource	Grants permission to list tags for a selected resource	Read	subscription-provider*		
RegisterSubscriptionProvider	Grants permission to create a new subscription provider in Amazon License Manager	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
TagResource	Grants permission to tag a selected resource	Tagging	subscription-provider*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a selected resource	Tagging	subscription-provider*		
				aws:TagKeys	
UpdateServiceSettings	Grants permission to update the service settings for Linux subscriptions in Amazon License Manager	Write			

Resource types defined by Amazon License Manager Linux Subscriptions 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
subscription-provider	`arn:${Partition}:license-manager-linux-subscriptions:${Region}:${Account}:subscription-provider/${SubscriptionProviderId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon License Manager Linux Subscriptions Manager

Amazon License Manager Linux Subscriptions 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 Amazon 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 tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by tag keys that are passed in the request	ArrayOfString

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 Amazon. 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.

> **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
DescribeVpcConnection	Grants permission to describe a MSK VPC connection	Read	vpc-connection*		
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListClustersV2	Grants permission to list all MSK clusters in this account	List			
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*		
ListVpcConnections	Grants permission to list all MSK VPC connections that this account uses	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
			vpc-connection		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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*		
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
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}
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}:${Account}:transactional-id/${ClusterNa`	

Resource types	ARN	Condition keys
	me}/${ClusterUuid}/${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 Amazon 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
kafka:publicAccessEnabled	Filters access by the presence of public access enabled in the request	Bool

Actions, resources, and condition keys for Amazon Managed Workflows for Apache Airflow

Amazon Managed Workflows for Apache Airflow (service prefix: `airflow`) 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 Workflows for Apache Airflow
- Resource types defined by Amazon Managed Workflows for Apache Airflow
- Condition keys for Amazon Managed Workflows for Apache Airflow

Actions defined by Amazon Managed Workflows for Apache Airflow

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 Amazon. 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.

> **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
CreateCliToken	Grants permission to create a short-lived token that allows a user to invoke Airflow CLI via an endpoint on the Apache Airflow Webserver	Write	environment*		
CreateEnvironment	Grants permission to create an Amazon MWAA environment	Write	environment*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateWebLoginToken	Grants permission to create a short-lived token that allows a user to log into Apache Airflow web UI	Write	rbac-role*		
DeleteEnvironment	Grants permission to delete an Amazon MWAA environment	Write	environment*		
				aws:ResourceTag/${TagKey}	
GetEnvironment	Grants permission to view details about an Amazon MWAA environment	Read	environment*		
				aws:ResourceTag/${TagKey}	
InvokeRestApi	Grants permission to invoke Airflow REST API via an endpoint on the Apache Airflow Webserver	Write	rbac-role*		
ListEnvironments	Grants permission to list the Amazon MWAA environments in your account	List			
ListTagsForResource	Grants permission to lists tag for an Amazon MWAA environment	Read	environment		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
PublishMetrics	Grants permission to publish metrics for an Amazon MWAA environment	Write	environment*		
TagResource	Grants permission to tag an Amazon MWAA environment	Tagging	environment		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to untag an Amazon MWAA environment	Tagging	environment		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateEnvironment	Grants permission to modify an Amazon MWAA environment	Write	environment*		
				aws:ResourceTag/${TagKey}	

Resource types defined by Amazon Managed Workflows for Apache Airflow

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
environment	`arn:${Partition}:airflow:${Region}:${Account}:environment/${EnvironmentName}`	

Resource types	ARN	Condition keys
rbac-role	`arn:${Partition}:airflow:${Region}:${Account}:role/${EnvironmentName}/${RoleName}`	

Condition keys for Amazon Managed Workflows for Apache Airflow

Amazon Managed Workflows for Apache Airflow 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 Amazon 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 tag keys in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Web Services Marketplace

Amazon Web Services Marketplace (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 Amazon Web Services Marketplace
- Resource types defined by Amazon Web Services Marketplace
- Condition keys for Amazon Web Services Marketplace

Actions defined by Amazon Web Services Marketplace

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 Amazon. 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.

> **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
AcceptAgreementApprovalRequest	Grants permission to users to approve an incoming subscription request (for providers who provide products that require subscription verification)	Write			
AcceptAgreementRequest	Grants permission to users to accept their agreement requests. Note that this action is not applicable to Marketplace purchases	Write			
CancelAgreement	Grants permission to users to cancel their agreements. Note that this action is not applicable to Marketplace purchases	Write			
CancelAgreementRequest	Grants permission to users to cancel pending subscription requests for products that	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	require subscription verification				
CreateAgreementRequest	Grants permission to users to create an agreement request. Note that this action is not applicable to Marketplace purchases	Write			
DescribeAgreement	Grants permission to users to describe the metadata about the agreement	Read			
GetAgreementApprovalRequest	Grants permission to users to view the details of their incoming subscription requests (for providers who provide products that require subscription verification)	Read			
GetAgreementEntitlements	Grants permission to users to view the entitlements associated with an agreement	Read			
GetAgreementRequest	Grants permission to users to view the details of their subscription requests for data products that require subscription verification	Read			
GetAgreementTerms	Grants permission to users to get a list of terms for an agreement	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAgreementApprovalRequests	Grants permission to users to list their incoming subscription requests (for providers who provide products that require subscription verification)	List			
ListAgreementCharges	Grants permission to users to view charges associated with their agreements	List			
ListAgreementRequests	Grants permission to users to list their subscription requests for products that require subscription verification	List			
ListEntitlementDetails	Grants permission to users to view details of the entitlements associated with an agreement. Note that this action is not applicable to Marketplace purchases	Read			
RejectAgreementApprovalRequest	Grants permission to users to decline an incoming subscription requests (for providers who provide products that require subscription verification)	Write			
SearchAgreements	Grants permission to users to search their agreements	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Subscribe	Grants permission to users to subscribe to Amazon Web Services Marketplace products. Includes the ability to send a subscription request for products that require subscription verification. Includes the ability to enable auto-renewal for an existing subscription	Write			
Unsubscribe	Grants permission to users to remove subscriptions to Amazon Web Services Marketplace products. Includes the ability to disable auto-renewal for an existing subscription	Write			
UpdateAgreementApprovalRequest	Grants permission to users to make changes to an incoming subscription request, including the ability to delete the prospective subscriber's information (for providers who provide products that require subscription verification)	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdatePurchaseOrders	Grants permission to users to update purchase orders for charges associated with their agreements	Write			
ViewSubscriptions	Grants permission to users to see their account's subscriptions	List			

Resource types defined by Amazon Web Services Marketplace

Amazon Web Services Marketplace does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon Web Services Marketplace, specify `"Resource": "*"` in your policy.

Condition keys for Amazon Web Services Marketplace

Amazon Web Services Marketplace 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 Amazon global condition context keys.

Condition keys	Description	Type
aws-marketplace:AgreementType	Filters access by the type of the agreement	ArrayOfString
aws-marketplace:PartyType	Filters access by the party type of the agreement	String

Condition keys	Description	Type
aws-marketplace:ProductId	Filters access by product id for Amazon Web Services Marketplace RedHat OpenShift and Bedrock Products. Note: Using this condition key will not restrict access to products in Amazon Web Services Marketplace	ArrayOfString

Actions, resources, and condition keys for Amazon Web Services Marketplace Entitlement Service

Amazon Web Services 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 Amazon Web Services Marketplace Entitlement Service
- Resource types defined by Amazon Web Services Marketplace Entitlement Service
- Condition keys for Amazon Web Services Marketplace Entitlement Service

Actions defined by Amazon Web Services 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 Amazon. 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.

> **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	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	customer identifier or product dimensions				

Resource types defined by Amazon Web Services Marketplace Entitlement Service

Amazon Web Services Marketplace Entitlement Service does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon Web Services Marketplace Entitlement Service, specify `"Resource": "*"` in your policy.

Condition keys for Amazon Web Services 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 Amazon global condition context keys.

Actions, resources, and condition keys for Amazon Web Services Marketplace Management Portal

Amazon Web Services Marketplace Management Portal (service prefix: `aws-marketplace-management`) 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 Web Services Marketplace Management Portal
- Resource types defined by Amazon Web Services Marketplace Management Portal
- Condition keys for Amazon Web Services Marketplace Management Portal

Actions defined by Amazon Web Services Marketplace Management Portal

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 Amazon. 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.

> **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
GetAdditionalSellerNotificationRecipients [permission only]	Grants permission to view additional seller notification recipients	Read			
GetBankAccountVerificationDetails [permission only]	Grants permission to view bank account verification status	Read			
GetSecondaryUserVerificationDetails [permission only]	Grants permission to view secondary user account verification status	Read			
GetSellerVerificationDetails [permission only]	Grants permission to view account verification status	Read			
PutAdditionalSellerNotificationRecip	Grants permission to update additional seller notification recipients	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ients [permission only]					
PutBankAccountVerificationDetails [permission only]	Grants permission to update bank account verification status	Write			
PutSecondaryUserVerificationDetails [permission only]	Grants permission to update secondary user account verification status	Write			
PutSellerVerificationDetails [permission only]	Grants permission to update account verification status	Write			
uploadFiles [permission only]	Allows access to the File Upload page inside the Amazon Web Services Marketplace Management Portal	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
viewMarketing [permission only]	Allows access to the Marketing page inside the Amazon Web Services Marketplace Management Portal	List			
viewReports [permission only]	Allows access to the Reports page inside the Amazon Web Services Marketplace Management Portal	List			
viewSettings [permission only]	Allows access to the Settings page inside the Amazon Web Services Marketplace Management Portal	List			
viewSupport [permission only]	Allows access to the Customer Support Eligibility page inside the Amazon Web Services Marketplace Management Portal	List			

Resource types defined by Amazon Web Services Marketplace Management Portal

Amazon Web Services Marketplace Management Portal does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon Web Services Marketplace Management Portal, specify `"Resource": "*"` in your policy.

Condition keys for Amazon Web Services Marketplace Management Portal

Marketplace Portal 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 Amazon global condition context keys.

Actions, resources, and condition keys for Amazon Web Services Marketplace Metering Service

Amazon Web Services 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 Amazon Web Services Marketplace Metering Service
- Resource types defined by Amazon Web Services Marketplace Metering Service
- Condition keys for Amazon Web Services Marketplace Metering Service

Actions defined by Amazon Web Services 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 Amazon. 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.

> **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 Amazon Web Services	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Marketplace, enabling you to guard against unauthorized use. Meters software use per ECS task, per 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 Amazon Web Services Marketplace Metering Service

Amazon Web Services Marketplace Metering Service does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon Web Services Marketplace Metering Service, specify `"Resource": "*"` in your policy.

Condition keys for Amazon Web Services 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 Amazon global condition context keys.

Actions, resources, and condition keys for Amazon MemoryDB

Amazon MemoryDB (service prefix: `memorydb`) 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 MemoryDB
- Resource types defined by Amazon MemoryDB
- Condition keys for Amazon MemoryDB

Actions defined by Amazon MemoryDB

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 Amazon. 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.

> **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**
>
> When you create a MemoryDB for Redis policy in IAM you must use the "*" wildcard character for the Resource block. For information about using the following MemoryDB for Redis API actions in an IAM policy, see MemoryDB Actions and IAM.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchUpdateCluster	Grants permissions to apply service updates	Write	cluster*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					s3:GetObject
				aws:ResourceTag/${TagKey}	
Connect	Allows an IAM user or role to connect as a specified MemoryDB user to a node in a cluster	Write	cluster*		
			user*		
				aws:ResourceTag/${TagKey}	
CopySnapshot	Grants permissions to make a copy of an existing snapshot	Write	snapshot*		memorydb:TagResource s3:DeleteObject s3:GetBucketAcl s3:PutObject

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateAcl	Grants permissions to create a new access control list	Write	user*		memorydb:TagResource
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCluster	Grants permissions to create a cluster	Write	acl*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs memorydb:TagResource s3:GetObject
			parametergroup*		
			subnetgroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			multiregioncluster		
			snapshot		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys memorydbTLSEnabled	
CreateMultiRegionCluster	Grants permissions to create a Multi-Region cluster	Write	multiregionparametergroup*		memorydb:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys memorydbTLSEnabled	
CreateParameterGroup	Grants permissions to create a new parameter group	Write		aws:RequestTag/${TagKey} aws:TagKeys	memorydb:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSnapshot	Grants permissions to create a backup of a cluster at the current point in time	Write	cluster*		memorydb:TagResource s3:DeleteObject s3:GetBucketAcl s3:PutObject
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateSubnetGroup	Grants permissions to create a new subnet group	Write		aws:RequestTag/${TagKey} aws:TagKeys	memorydb:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateUser	Grants permissions to create a new user	Write		aws:RequestTag/${TagKey} aws:TagKeys memorydbUserAuthenticationMode	memorydb:TagResource
DeleteAcl	Grants permissions to delete an access control list	Write	acl*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteCluster	Grants permissions to delete a previously provisioned cluster	Write	cluster*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
			multiregioncluster		
			snapshot		
				aws:ResourceTag/${TagKey}	
DeleteMultiRegionCluster	Grants permissions to delete a Multi-Region cluster	Write	multiregioncluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
DeleteParameterGroup	Grants permissions to delete a parameter group	Write	parameter group*		
				aws:ResourceTag/${TagKey}	
DeleteSnapshot	Grants permissions to delete a snapshot	Write	snapshot*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteSubnetGroup	Grants permissions to delete a subnet group	Write	subnetgroup*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey}	
DeleteUser	Grants permissions to delete a user	Write	user*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeAcls	Grants permissions to retrieve information about access control lists	Read	acl*		
				aws:ResourceTag/${TagKey}	
DescribeClusters	Grants permissions to retrieve information about all provisioned clusters if no cluster identifier is specified, or about a specific cluster if a cluster identifier is supplied	Read	cluster*		
				aws:ResourceTag/${TagKey}	
DescribeEngineVersions	Grants permissions to list of the available engines and their versions	Read			
DescribeEvents	Grants permissions to retrieve events related to clusters, subnet groups, and parameter groups	Read			
DescribeMultiRegionClusters	Grants permissions to retrieve information about all Multi-Region clusters if no cluster identifier is specified, or about a specific Multi-Region cluster if a cluster identifier is supplied	Read	multiregioncluster*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeMultiRegionParameterGroups	Grants permissions to retrieve information about Multi-Region parameter groups	Read	multiregionparametergroup*		
DescribeMultiRegionParameters	Grants permissions to retrieve a detailed parameter list for a particular Multi-Region parameter group	Read	multiregionparametergroup*		
DescribeParameterGroups	Grants permissions to retrieve information about parameter groups	Read	parametergroup*		
				aws:ResourceTag/${TagKey}	
DescribeParameters	Grants permissions to retrieve a detailed parameter list for a particular parameter group	Read	parametergroup*		
				aws:ResourceTag/${TagKey}	
DescribeReservedNodes	Grants permissions to retrieve reserved nodes	Read	reservednode*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeReservedNodesOfferings	Grants permissions to retrieve reserved nodes offerings	Read			
DescribeServiceUpdates	Grants permissions to retrieve details of the service updates	Read			
DescribeSnapshots	Grants permissions to retrieve information about cluster snapshots	Read	snapshot*		
				aws:ResourceTag/${TagKey}	
DescribeSubnetGroups	Grants permissions to retrieve a list of subnet group	Read	subnetgroup*		
				aws:ResourceTag/${TagKey}	
DescribeUsers	Grants permissions to retrieve information about users	Read	user*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
FailoverShard	Grants permissions to test automatic failover on a specified shard in a cluster	Write	cluster*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
				aws:ResourceTag/${TagKey}	
ListAllowedMultiRegionClusterUpdates	Grants permissions to list available Multi-Region cluster updates	Read	multiregioncluster*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAllowedNodeTypeUpdates	Grants permissions to list available node type updates	Read	cluster*		
				aws:ResourceTag/${TagKey}	
ListTags	Grants permissions to list cost allocation tags	Read	acl		
			cluster		
			multiregioncluster		
			parametergroup		
			snapshot		
			subnetgroup		
			user		
				aws:ResourceTag/${TagKey}	
PurchaseReservedNodesOffering	Grants permissions to purchase a new reserved node	Write	reservednode*		memorydb:TagResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
ResetParameterGroup	Grants permissions to modify the parameters of a parameter group to the engine or system default value	Write	parametergroup*		
				aws:ResourceTag/${TagKey}	
TagResource	Grants permissions to add up to 10 cost allocation tags to the named resource	Tagging	acl		
			cluster		
			multiregioncluster		
			parametergroup		
			reservednode		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot		
			subnetgroup		
			user		
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permissions to remove the tags identified by the TagKeys list from a resource	Tagging	acl		
			cluster		
			multiregioncluster		
			parametergroup		
			snapshot		
			subnetgroup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			user		
				aws:TagKeys aws:ResourceTag/${TagKey}	
UpdateAcl	Grants permissions to update an access control list	Write	acl*		
			user*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateCluster	Grants permissions to update the settings for a cluster	Write	cluster*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
			acl		
			parameter group		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateMultiRegionCluster	Grants permissions to update the settings for a Multi-Region cluster	Write	multiregioncluster*		ec2:CreateNetworkInterface ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:DescribeVpcs
			multiregionparametergroup		
				aws:ResourceTag/${TagKey}	
UpdateParameterGroup	Grants permissions to update parameters in a parameter group	Write	parametergroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
UpdateSubnetGroup	Grants permissions to update a subnet group	Write	subnetgroup*		
				aws:ResourceTag/${TagKey}	
UpdateUser	Grants permissions to update a user	Write	user*		
				aws:ResourceTag/${TagKey} memorydbUserAuthenticationMode	

Resource types defined by Amazon MemoryDB

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
multiregionparametergroup	arn:${Partition}:memorydb::${Account}:multiregionparametergroup/${MultiRegionParameterGroupName}	
parametergroup	arn:${Partition}:memorydb:${Region}:${Account}:parametergroup/${ParameterGroupName}	aws:ResourceTag/${TagKey}
subnetgroup	arn:${Partition}:memorydb:${Region}:${Account}:subnetgroup/${SubnetGroupName}	aws:ResourceTag/${TagKey}
multiregioncluster	arn:${Partition}:memorydb::${Account}:multiregioncluster/${ClusterName}	aws:ResourceTag/${TagKey} memorydb:TLSEnabled
cluster	arn:${Partition}:memorydb:${Region}:${Account}:cluster/${ClusterName}	aws:ResourceTag/${TagKey}
snapshot	arn:${Partition}:memorydb:${Region}:${Account}:snapshot/${SnapshotName}	aws:ResourceTag/${TagKey}
user	arn:${Partition}:memorydb:${Region}:${Account}:user/${UserName}	aws:ResourceTag/${TagKey}
acl	arn:${Partition}:memorydb:${Region}:${Account}:acl/${AclName}	aws:ResourceTag/${TagKey}
reservednode	arn:${Partition}:memorydb:${Region}:${Account}:reservednode/${ReservationID}	aws:ResourceTag/${TagKey}

Condition keys for Amazon MemoryDB

Amazon MemoryDB 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 Amazon global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters actions based on the tags that are passed in the request	String
aws:ResourceTag/${TagKey}	Filters actions based on the tags associated with the resource	String
aws:TagKeys	Filters actions based on the tag keys that are passed in the request	ArrayOfString
memorydb:TLSEnabled	Filters access by the TLSEnabled parameter present in the request or defaults to true value if parameter is not present	Bool
memorydb:UserAuthenticationMode	Filters access by the UserAuthenticationMode.Type parameter in the request	String

Actions, resources, and condition keys for Amazon Message Delivery Service

Amazon Message Delivery Service (service prefix: `ec2messages`) 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 Message Delivery Service
- Resource types defined by Amazon Message Delivery Service
- Condition keys for Amazon Message Delivery Service

Actions defined by Amazon Message Delivery 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 Amazon. 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.

> **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
AcknowledgeMessage	Grants permission to acknowledge a message, ensuring it will not be delivered again	Write			
DeleteMessage	Grants permission to delete a message	Write			
FailMessage	Grants permission to fail a message, signifying the message could not be processed successfully, ensuring it cannot be replied to or delivered again	Write			
GetEndpoint	Grants permission to route traffic to the correct endpoint based on the given destination for the messages	Read			
GetMessages	Grants permission to deliver messages to clients/instances using long polling	Read		ssm:SourceInstanceARN	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ec2:SourceInstanceARN	
SendReply	Grants permission to send replies from clients/instances to upstream service	Write		ssm:SourceInstanceARN ec2:SourceInstanceARN	

Resource types defined by Amazon Message Delivery Service

Amazon Message Delivery Service does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon Message Delivery Service, specify `"Resource": "*"` in your policy.

Condition keys for Amazon Message Delivery Service

Amazon Message Delivery 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 Amazon global condition context keys.

Condition keys	Description	Type
ec2:SourceInstanceARN	Filters access by the ARN of the instance from which the request originated	ARN

Condition keys	Description	Type
ssm:SourceInstanceARN	Filters access by verifying the Amazon Resource Name (ARN) of the Amazon Systems Manager's managed instance from which the request is made. This key is not present when the request comes from the managed instance authenticated with an IAM role associated with EC2 instance profile	ARN

Actions, resources, and condition keys for Amazon Message Gateway Service

Amazon Message Gateway Service (service prefix: `ssmmessages`) 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 Message Gateway Service
- Resource types defined by Amazon Message Gateway Service
- Condition keys for Amazon Message Gateway Service

Actions defined by Amazon Message Gateway 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 Amazon. 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.

> **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
CreateControlChannel	Grants permission to register a control channel for an instance to send control	Write		ssm:SourceInstanceARN	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	messages to Systems Manager service			ec2:SourceInstanceARN	
CreateDataChannel	Grants permission to register a data channel for an instance to send data messages to Systems Manager service	Write			
OpenControlChannel	Grants permission to open a websocket connection for a registered control channel stream from an instance to Systems Manager service	Write			
OpenDataChannel	Grants permission to open a websocket connection for a registered data channel stream from an instance to Systems Manager service	Write			

Resource types defined by Amazon Message Gateway Service

Amazon Message Gateway Service does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon Message Gateway Service, specify `"Resource": "*"` in your policy.

Condition keys for Amazon Message Gateway Service

Amazon Message Gateway 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 Amazon global condition context keys.

Condition keys	Description	Type
ec2:SourceInstanceARN	Filters access by the ARN of the instance from which the request originated	ARN
ssm:SourceInstanceARN	Filters access by verifying the Amazon Resource Name (ARN) of the Amazon Systems Manager's managed instance from which the request is made. This key is not present when the request comes from the managed instance authenticated with an IAM role associated with EC2 instance profile	ARN

Actions, resources, and condition keys for Amazon MQ

Amazon MQ (service prefix: `mq`) 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 MQ
- Resource types defined by Amazon MQ
- Condition keys for Amazon MQ

Actions defined by Amazon MQ

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 Amazon. 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.

> **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
CreateBroker	Grants permission to create a broker	Write		aws:RequestTag/${TagKey} aws:TagKeys	ec2:CreateNetworkInterface ec2:CreateNetworkInterfacePermission ec2:CreateSecurityGroup ec2:CreateVpcEndpoint ec2:DescribeInternetGateways ec2:DescribeNetworkInterfacePermissions ec2:DescribeNetworkInterfaces

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcEndpoints ec2:DescribeVpcs ec2:ModifyNetworkInterfaceAttribute iam:CreateServiceLinkedRole route53:AssociateVPCWithHostedZone

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateConfiguration	Grants permission to create a new configuration for the specified configuration name. Amazon MQ uses the default configuration (the engine type and engine version)	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateReplicaBroker [permission only]	Grants permission to create a replica broker	Write	brokers*		
CreateTags	Grants permission to create tags	Tagging	brokers		
			configurations		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUser	Grants permission to create an ActiveMQ user	Write	brokers*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteBroker	Grants permission to delete a broker	Write	brokers*		ec2:DeleteNetworkInterface ec2:DeleteNetworkInterfacePermission ec2:DeleteVpcEndpoints ec2:DetachNetworkInterface
DeleteConfiguration	Grants permission to delete a configuration	Write	configurations*		
DeleteTags	Grants permission to delete tags	Tagging	brokers		
			configurations		
				aws:TagKeys	
DeleteUser	Grants permission to delete an ActiveMQ user	Write	brokers*		
DescribeBroker	Grants permission to return information about the specified broker	Read	brokers*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeBrokerEngineTypes	Grants permission to return information about broker engines	Read			
DescribeBrokerInstanceOptions	Grants permission to return information about the broker instance options	Read			
DescribeConfiguration	Grants permission to return information about the specified configuration	Read	configurations*		
DescribeConfigurationRevision	Grants permission to return the specified configuration revision for the specified configuration	Read	configurations*		
DescribeUser	Grants permission to return information about an ActiveMQ user	Read	brokers*		
ListBrokers	Grants permission to return a list of all brokers	List			
ListConfigurationRevisions	Grants permission to return a list of all existing revisions for the specified configuration	List	configurations*		
ListConfigurations	Grants permission to return a list of all configurations	List			
ListTags	Grants permission to return a list of tags	List	brokers		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			configurations		
ListUsers	Grants permission to return a list of all ActiveMQ users	List	brokers*		
Promote	Grants permission to promote a broker	Write	brokers*		
RebootBroker	Grants permission to reboot a broker	Write	brokers*		
UpdateBroker	Grants permission to add a pending configuration change to a broker	Write	brokers*		
UpdateConfiguration	Grants permission to update the specified configuration	Write	configurations*		
UpdateUser	Grants permission to update the information for an ActiveMQ user	Write	brokers*		

Resource types defined by Amazon MQ

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
brokers	`arn:${Partition}:mq:${Region}:${Account}:broker:${BrokerName}:${BrokerId}`	aws:ResourceTag/${TagKey}
configurations	`arn:${Partition}:mq:${Region}:${Account}:configuration:${ConfigurationId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon MQ

Amazon MQ 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 Amazon 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 Neptune

Amazon Neptune (service prefix: `neptune-db`) 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 Neptune
- Resource types defined by Amazon Neptune
- Condition keys for Amazon Neptune

Actions defined by Amazon Neptune

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 Amazon. 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.

> **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
CancelLoaderJob	Grants permission to cancel a loader job	Write	database*		
CancelMLDataProcessingJob	Grants permission to cancel an ML data processing job	Write	database*		
CancelMLModelTrainingJob	Grants permission to cancel an ML model training job	Write	database*		
CancelMLModelTransformJob	Grants permission to cancel an ML model transform job	Write	database*		
CancelQuery	Grants permission to cancel a query	Write	database*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateMLEndpoint	Grants permission to create an ML endpoint	Write	database*		
DeleteDataViaQuery	Grants permission to run delete data via query APIs on database	Write	database*		
				neptune-db:QueryLanguage	
DeleteMLEndpoint	Grants permission to delete an ML endpoint	Write	database*		
DeleteStatistics	Grants permission to delete all the statistics in the database	Write	database*		
GetEngineStatus	Grants permission to check the status of the Neptune engine	Read	database*		
GetGraphSummary	Grants permission to get the graph summary from the database	Read	database*		
GetLoaderJobStatus	Grants permission to check the status of a loader job	Read	database*		
GetMLDataProcessingJobStatus	Grants permission to check the status of an ML data processing job	Read	database*		
GetMLEndpointStatus	Grants permission to check the status of an ML endpoint	Read	database*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetMLModelTrainingJobStatus	Grants permission to check the status of an ML model training job	Read	database*		
GetMLModelTransformJobStatus	Grants permission to check the status of an ML model transform job	Read	database*		
GetQueryStatus	Grants permission to check the status of all active queries	Read	database*		
				neptune-db:QueryLanguage	
GetStatisticsStatus	Grants permission to check the status of statistics of the database	Read	database*		
GetStreamRecords	Grants permission to fetch stream records from Neptune	Read	database*		
				neptune-db:QueryLanguage	
ListLoaderJobs	Grants permission to list all the loader jobs	List	database*		
ListMLDataProcessingJobs	Grants permission to list all the ML data processing jobs	List	database*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListMLEndpoints	Grants permission to list all the ML endpoints	List	database*		
ListMLModelTrainingJobs	Grants permission to list all the ML model training jobs	List	database*		
ListMLModelTransformJobs	Grants permission to list all the ML model transform jobs	List	database*		
ManageStatistics	Grants permission to manage statistics in the database	Write	database*		
ReadDataViaQuery	Grants permission to run read data via query APIs on database	Read	database*		
				neptune-db:QueryLanguage	
ResetDatabase	Grants permission to get the token needed for reset and resets the Neptune database	Write	database*		
StartLoaderJob	Grants permission to start a loader job	Write	database*		
StartMLDataProcessingJob	Grants permission to start an ML data processing job	Write	database*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartMLModelTrainingJob	Grants permission to start an ML model training job	Write	database*		
StartMLModelTransformJob	Grants permission to start an ML model transform job	Write	database*		
WriteDataViaQuery	Grants permission to run write data via query APIs on database	Write	database*		
				neptune-db:QueryLanguage	
connect	Grants permission to all data-access actions in engine versions prior to 1.2.0.0	Write	database*		

Resource types defined by Amazon Neptune

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
database	`arn:${Partition}:neptune-db:${Region}:${Account}:${ClusterResourceId}/*`	

Condition keys for Amazon Neptune

Amazon Neptune 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 Amazon global condition context keys.

Condition keys	Description	Type
neptune-db:QueryLanguage	Filters access by graph model	String

Actions, resources, and condition keys for Amazon Network Firewall

Amazon Network Firewall (service prefix: `network-firewall`) 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 Network Firewall
- Resource types defined by Amazon Network Firewall
- Condition keys for Amazon Network Firewall

Actions defined by Amazon Network Firewall

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 Amazon. 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.

> **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 FirewallPolicy	Grants permission to create an association between a firewall policy and a firewall	Write	Firewall*		
			FirewallPolicy*		
Associate Subnets	Grants permission to associate VPC subnets to a firewall	Write	Firewall*		
CreateFirewall	Grants permission to create an Amazon Network Firewall firewall	Write	Firewall*		iam:CreateServiceLinkedRole
			FirewallPolicy*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFirewallPolicy	Grants permission to create an Amazon Network Firewall firewall policy	Write	FirewallPolicy*		
			StatefulRuleGroup		
			StatelessRuleGroup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			TLSInspectionConfiguration		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRuleGroup	Grants permission to create an Amazon Network Firewall rule group	Write	StatefulRuleGroup		
			StatelessRuleGroup		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTLSInspectionConfiguration	Grants permission to create an Amazon Network Firewall tls inspection configuration	Write	TLSInspectionConfiguration*		iam:CreateServiceLinkedRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteFirewall	Grants permission to delete a firewall	Write	Firewall*		
DeleteFirewallPolicy	Grants permission to delete a firewall policy	Write	FirewallPolicy*		
DeleteResourcePolicy	Grants permission to delete a resource policy for a firewall policy or rule group	Write	FirewallPolicy		
			StatefulRuleGroup		
			StatelessRuleGroup		
DeleteRuleGroup	Grants permission to delete a rule group	Write	StatefulRuleGroup*		
			StatelessRuleGroup*		
DeleteTLSInspectionConfiguration	Grants permission to delete a tls inspection configuration	Write	TLSInspectionConfiguration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeFirewall	Grants permission to retrieve the data objects that define a firewall	Read	Firewall*		
DescribeFirewallPolicy	Grants permission to retrieve the data objects that define a firewall policy	Read	FirewallPolicy*		
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		
DescribeFlowOperation	Grants permission to describe a flow operation performed on a firewall	Read	Firewall*		
DescribeLoggingConfiguration	Grants permission to describe the logging configuration of a firewall	Read	Firewall*		logs:GetLogDelivery logs:ListLogDeliveries
DescribeResourcePolicy	Grants permission to describe a resource policy for a firewall policy or rule group	Read	FirewallPolicy		
			StatefulRuleGroup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			StatelessRuleGroup		
DescribeRuleGroup	Grants permission to retrieve the data objects that define a rule group	Read	StatefulRuleGroup		
			StatelessRuleGroup		
DescribeRuleGroupMetadata	Grants permission to retrieve the high-level information about a rule group	Read	StatefulRuleGroup		
			StatelessRuleGroup		
DescribeTLSInspectionConfiguration	Grants permission to retrieve the data objects that define a tls inspection configuration	Read	TLSInspectionConfiguration*		
DisassociateSubnets	Grants permission to disassociate VPC subnets from a firewall	Write	Firewall*		
GetAnalysisReportResults	Grants permission to retrieve analysis report results of a firewall	Read	Firewall*		
ListAnalysisReports	Grants permission to list firewall analysis reports	List	Firewall*		
ListFirewallPolicies	Grants permission to retrieve the metadata for firewall policies	List	FirewallPolicy*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListFirewalls	Grants permission to retrieve the metadata for firewalls	List	Firewall*		
ListFlowOperationResults	Grants permission to list results from a flow operation performed on a firewall	Read	Firewall*		
ListFlowOperations	Grants permission to list flow operations performed on a firewall	List	Firewall*		
ListRuleGroups	Grants permission to retrieve the metadata for rule groups	List			
ListTLSInspectionConfigurations	Grants permission to retrieve the metadata for tls inspection configurations	List	TLSInspectionConfiguration*		
ListTagsForResource	Grants permission to retrieve the tags for a resource	List	Firewall*		
			FirewallPolicy*		
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutResourcePolicy	Grants permission to put a resource policy for a firewall policy or rule group	Write	FirewallPolicy		
			StatefulRuleGroup		
			StatelessRuleGroup		
StartAnalysisReport	Grants permission to start an analysis report on a firewall	Write	Firewall*		
StartFlowCapture	Grants permission to start capture operation on a firewall	Write	Firewall*		
StartFlowFlush	Grants permission to start flush operation on a firewall	Write	Firewall*		
TagResource	Grants permission to attach tags to a resource	Tagging	Firewall		
			FirewallPolicy		
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove tags from a resource	Tagging	Firewall		
			FirewallPolicy		
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		
				aws:TagKeys	
UpdateFirewallAnalysisSettings	Grants permission to modify firewall analysis settings of a firewall	Write	Firewall*		
UpdateFirewallDeleteProtection	Grants permission to add or remove delete protection for a firewall	Write	Firewall*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateFirewallDescription	Grants permission to modify the description for a firewall	Write	Firewall*		
UpdateFirewallEncryptionConfiguration	Grants permission to modify the encryption configuration of a firewall	Write	Firewall*		
UpdateFirewallPolicy	Grants permission to modify a firewall policy	Write	FirewallPolicy*		
			StatefulRuleGroup		
			StatelessRuleGroup		
			TLSInspectionConfiguration		
UpdateFirewallPolicyChangeProtection	Grants permission to add or remove firewall policy change protection for a firewall	Write	Firewall*		
UpdateLoggingConfiguration	Grants permission to modify the logging configuration of a firewall	Write	Firewall*		
UpdateRuleGroup	Grants permission to modify a rule group	Write	StatefulRuleGroup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			StatelessRuleGroup		
UpdateSubnetChangeProtection	Grants permission to add or remove subnet change protection for a firewall	Write	Firewall*		
UpdateTLSInspectionConfiguration	Grants permission to modify a tls inspection configuration	Write	TLSInspectionConfiguration*		

Resource types defined by Amazon Network Firewall

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
Firewall	`arn:${Partition}:network-firewall:${Region}:${Account}:firewall/${Name}`	aws:ResourceTag/${TagKey}
FirewallPolicy	`arn:${Partition}:network-firewall:${Region}:${Account}:firewall-policy/${Name}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
StatefulRuleGroup	`arn:${Partition}:network-firewall:${Region}:${Account}:stateful-rulegroup/${Name}`	aws:ResourceTag/${TagKey}
StatelessRuleGroup	`arn:${Partition}:network-firewall:${Region}:${Account}:stateless-rulegroup/${Name}`	aws:ResourceTag/${TagKey}
TLSInspectionConfiguration	`arn:${Partition}:network-firewall:${Region}:${Account}:tls-configuration/${Name}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Network Firewall

Amazon Network Firewall 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 Amazon global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by on the allowed set of values for each of the tags	String
aws:ResourceTag/${TagKey}	Filters access by the 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 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 Amazon. 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.

> **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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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/${TagKey} aws:TagKeys	
AddTags	Grants permission to attach resource tags to an OpenSearch Service domain, data source, or application	Tagging	application*		
			datasource*		
			domain*		
				aws:RequestTag/${TagKey} aws:TagKeys	
AssociatePackage	Grants permission to associate a package with an OpenSearch Service domain	Write	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Associate Packages	Grants permission to associate multiple packages with an OpenSearch Service domain	Write	domain*		
Authorize VpcEndpointAccess	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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDomain	Grants permission to create an Amazon OpenSearch Service domain	Write	domain		
				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			

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			
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			
DeleteVpcEndpoint	Grants permission to delete an Amazon OpenSearch Service-managed interface VPC endpoint	Write			

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
DescribeInboundConnections	Grants permission to list all the inbound cross-cluster search connections for a destination domain	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
DescribePackages	Grants permission to describe all packages available to OpenSearch Service domains	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
DescribeVpcEndpoints	Grants permission to describe one or more Amazon OpenSearch Service-managed VPC endpoints	List			

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetDomainMaintenanceStatus	Grants permission to retrieve the status of maintenance action for the node	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*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
ListElasticsearchVersions	Grants permission to list all supported OpenSearch versions on Amazon OpenSearch Service. This permission is deprecated. Use ListVersions instead	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
ListVersions	Grants permission to list all supported OpenSearch and Elasticsearch versions in Amazon OpenSearch Service	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListVpcEndpointAccess	Grants permission to retrieve information about each Amazon 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 Amazon Web Services 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			
PurchaseReservedInstanceOffering	Grants permission to purchase OpenSearch reserved instances	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	
RevokeVpcEndpointAccess	Grants permission to revoke access to an Amazon OpenSearch Service domain that was provided through an interface VPC endpoint	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
UpdateDomainConfig	Grants permission to modify the configuration of an OpenSearch Service domain, such as the instance type or number of instances	Write	domain*		

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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/${TagKey}
application	`arn:${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::${Account}:role/aws-service-role/opensearchservice`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
	`.amazonaws.com/AWSServiceRoleForAmazonOpenSearchService`	
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 Amazon 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

Actions, resources, and condition keys for Amazon Organizations

Amazon 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 Amazon Organizations
- Resource types defined by Amazon Organizations
- Condition keys for Amazon Organizations

Actions defined by Amazon 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 Amazon. 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.

> **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 Amazon Web Services	Write	account*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	account that is now a part of an Organizations, either created within the organization, or invited to join the organization				
CreateAccount	Grants permission to create an Amazon Web Services account that is automatically a member of the organization with the credentials that made the request	Write		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	
CreateGovCloudAccount	Grants permission to create an Amazon GovCloud (US) account	Write		aws:RequestTag/${TagKey} aws:TagKeys aws:ResourceTag/${TagKey}	

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePolicy	Grants permission to create a policy that you can attach to a root, an organizational unit (OU), or an individual Amazon Web Services 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			
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				organizations:PolicyType	
DeleteResourcePolicy	Grants permission to delete a resource policy from your organization	Write			
DeregisterDelegatedAdministrator	Grants permission to deregister the specified member Amazon Web Services account as a delegated administrator for the Amazon 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*		
				organizations:PolicyType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeHandshake	Grants permission to retrieve details about a previously requested handshake	Read	handshake*		
DescribeOrganization	Grants permission to retrieves 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 retrieves details about a policy	Read	policy*		
				organizations:PolicyType	
DescribeResourcePolicy	Grants permission to retrieve information about a resource policy	Read			
DetachPolicy	Grants permission to detach a policy from a target root, organizational unit, or account	Write	policy*		
			account		
			organizationalunit		
			root		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				organizations:PolicyType	
DisableAWSServiceAccess	Grants permission to disable integration of an Amazon service (the service that is specified by ServicePrincipal) with Amazon Organizations	Write		organizations:ServicePrincipal	
DisablePolicyType	Grants permission to disable an organization policy type in a root	Write	root*		
				organizations:PolicyType	
EnableAWSServiceAccess	Grants permission to enable integration of an Amazon service (the service that is specified by ServicePrincipal) with Amazon 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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				organizations:PolicyType	
InviteAccountToOrganization	Grants permission to send an invitation to another Amazon Web Services account, asking it to join your organization as a member account	Write	account		
				aws:RequestTag/${TagKey} aws:TagKeys	
LeaveOrganization	Grants permission to remove a member account from its parent organization	Write			
ListAWSServiceAccessForOrganization	Grants permission to retrieve the list of the Amazon services for which you enabled integration with your organization	List			
ListAccounts	Grants permission to list all of the 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		

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 Amazon accounts that are designated as delegated administrators in this organization	List		organizations:ServicePrincipal	
ListDelegatedServicesForAccount	Grants permission to list the Amazon services for which the specified account is a delegated administrator in this organization	List	account*		
ListHandshakesForAccount	Grants permission to list all of the handshakes that are associated with an account	List			
ListHandshakesForOrganization	Grants permission to list the handshakes that are associated with the organization	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListOrganizationalUnitsForParent	Grants permission to lists all of the organizational units (OUs) in a parent organizational unit or root	List	organizationalunit		
			root		
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		
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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			policy		
			resourcepolicy		
			root		
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 Amazon service that is specified by ServicePrincipal	Write	account*		
				organizations:ServicePrincipal	
RemoveAccountFromOrganization	Grants permission to removes 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		
			root		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagResource	Grants permission to remove one or more tags from the specified resource	Tagging	account		
			organizationalunit		
			policy		
			resourcepolicy		
			root		
				aws:TagKeys	
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	

Resource types defined by Amazon 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-${OrganizationId}	
organizationalunit	arn:${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}

Condition keys for Amazon Organizations

Amazon 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 Amazon 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

Actions, resources, and condition keys for Amazon Payments

Amazon Payments (service prefix: `payments`) 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 Payments

- Resource types defined by Amazon Payments
- Condition keys for Amazon Payments

Actions defined by Amazon Payments

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 Amazon. 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.

> **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
AcceptFinancingApplicationTerms	Grants permission to accept financing application terms provided by a lender	Write			
CreateFinancingApplication	Grants permission to create a financing application	Write			
CreatePaymentInstrument	Grants permission to create a payment instrument	Write		aws:TagKeys aws:RequestTag/${TagKey}	
DeletePaymentInstrument [permission only]	Grants permission to delete a payment instrument	Write			
GetFinancingApplication	Grants permission to get information about a financing application	Read			
GetFinancingLine	Grants permission to get information about a financing line	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetFinancingLineWithdrawal	Grants permission to get information about a financing line withdrawal	Read			
GetFinancingOption	Grants permission to get information about a financing option	Read			
GetPaymentInstrument	Grants permission to get information about a payment instrument	List	payment-instrument		
GetPaymentStatus [permission only]	Grants permission to get payment status of invoices	Read			
ListFinancingApplications	Grants permission to list financing application metadata	List			
ListFinancingLineWithdrawals	Grants permission to list financing line withdrawals metadata	List			
ListFinancingLines	Grants permission to list financing line metadata	List			
ListPaymentInstruments [permission only]	Grants permission to list payment instrument metadata	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPaymentPreferences [permission only]	Grants permission to get payment preferences (preferred payment currency, preferred payment method, etc.)	List			
ListPaymentProgramOptions	Grants permission to list information about payment options	List			
ListPaymentProgramStatus	Grants permission to list information about payment program eligibility and enrolment status	List			
ListTagsForResource	Grants permission to list tags on a payment resource	List	payment-instrument		
MakePayment [permission only]	Grants permission to make a payment, authenticate a payment, verify a payment method, and generate a funding request document for Advance Pay	Write			
TagResource	Grants permission to tag a payment resource	Tagging	payment-instrument		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to untag a payment resource	Tagging	payment-instrument		
				aws:TagKeys	
UpdateFinancingApplication	Grants permission to update a financing application	Write			
UpdatePaymentInstrument [permission only]	Grants permission to update a payment instrument	Write			
UpdatePaymentPreferences [permission only]	Grants permission to update payment preferences (preferred payment currency, preferred payment method, etc.)	Write			

Resource types defined by Amazon Payments

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
payment-instrument	`arn:${Partition}:payments::${Account}:payment-instrument:${ResourceId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Payments

Amazon Payments 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 Amazon 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 Performance Insights

Amazon 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 Amazon Performance Insights
- Resource types defined by Amazon Performance Insights
- Condition keys for Amazon Performance Insights

Actions defined by Amazon 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 Amazon. 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.

> **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	Write	perf-reports-resource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Performance Analysis Report for a specified DB instance				
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	
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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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	perf-reports-resource*		
TagResource	Grants permission to call TagResource API to tag a resource	Tagging	perf-reports-resource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to call UntagResource API to untag a resource	Tagging	perf-reports-resource*		
				aws:TagKeys	

Resource types defined by Amazon 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}`	

Resource types	ARN	Condition keys
perf-reports-resource	`arn:${Partition}:pi:${Region}:${Account}:perf-reports/${ServiceType}/${Identifier}/${ReportId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Performance Insights

Amazon 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 Amazon 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 Amazon Personalize

Amazon Personalize (service prefix: `personalize`) 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 Personalize
- Resource types defined by Amazon Personalize
- Condition keys for Amazon Personalize

Actions defined by Amazon Personalize

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 Amazon. 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.

> **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
CreateBatchInferenceJob	Grants permission to create a batch inference job	Write	batchInferenceJob*		
CreateBatchSegmentJob	Grants permission to create a batch segment job	Write	batchSegmentJob*		
CreateCampaign	Grants permission to create a campaign	Write	campaign*		
CreateDataDeletionJob	Grants permission to create a data deletion job	Write	dataDeletionJob*		
CreateDataInsightsJob	Grants permission to create a data insights job	Write	dataInsightsJob*		
CreateDataset	Grants permission to create a dataset	Write	dataset*		
CreateDatasetExportJob	Grants permission to create a dataset export job	Write	datasetExportJob*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDatasetGroup	Grants permission to create a dataset group	Write	datasetGroup*		
CreateDatasetImportJob	Grants permission to create a dataset import job	Write	datasetImportJob*		
CreateEventTracker	Grants permission to create an event tracker	Write	eventTracker*		
CreateFilter	Grants permission to create a filter	Write	filter*		
CreateMetricAttribution	Grants permission to create a metric attribution	Write	metricAttribution*		
CreateRecommender	Grants permission to create a recommender	Write	recommender*		
CreateSchema	Grants permission to create a schema	Write	schema*		
CreateSolution	Grants permission to create a solution	Write	solution*		
CreateSolutionVersion	Grants permission to create a solution version	Write	solution*		
DeleteCampaign	Grants permission to delete a campaign	Write	campaign*		
DeleteDataset	Grants permission to delete a dataset	Write	dataset*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteDatasetGroup	Grants permission to delete a dataset group	Write	datasetGroup*		
DeleteEventTracker	Grants permission to delete an event tracker	Write	eventTracker*		
DeleteFilter	Grants permission to delete a filter	Write	filter*		
DeleteMetricAttribution	Grants permission to delete a metric attribution	Write	metricAttribution*		
DeleteRecommender	Grants permission to delete a recommender	Write	recommender*		
DeleteSchema	Grants permission to delete a schema	Write	schema*		
DeleteSolution	Grants permission to delete a solution including all versions of the solution	Write	solution*		
DescribeAlgorithm	Grants permission to describe an algorithm	Read	algorithm*		
DescribeBatchInferenceJob	Grants permission to describe a batch inference job	Read	batchInferenceJob*		
DescribeBatchSegmentJob	Grants permission to describe a batch segment job	Read	batchSegmentJob*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeCampaign	Grants permission to describe a campaign	Read	campaign*		
DescribeDataDeletionJob	Grants permission to describe a data deletion job	Read	dataDeletionJob*		
DescribeDataInsightsJob	Grants permission to describe a data insights job	Read	dataInsightsJob*		
DescribeDataset	Grants permission to describe a dataset	Read	dataset*		
DescribeDatasetExportJob	Grants permission to describe a dataset export job	Read	datasetExportJob*		
DescribeDatasetGroup	Grants permission to describe a dataset group	Read	datasetGroup*		
DescribeDatasetImportJob	Grants permission to describe a dataset import job	Read	datasetImportJob*		
DescribeEventTracker	Grants permission to describe an event tracker	Read	eventTracker*		
DescribeFeatureTransformation	Grants permission to describe a feature transformation	Read	featureTransformation*		
DescribeFilter	Grants permission to describe a filter	Read	filter*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeMetricAttribution	Grants permission to describe a metric attribution	Read	metricAttribution*		
DescribeRecipe	Grants permission to describe a recipe	Read	recipe*		
DescribeRecommender	Grants permission to describe a recommender	Read	recommender*		
DescribeSchema	Grants permission to describe a schema	Read	schema*		
DescribeSolution	Grants permission to describe a solution	Read	solution*		
DescribeSolutionVersion	Grants permission to describe a version of a solution	Read	solution*		
GetActionRecommendations	Grants permission to get a list of recommended actions	Read	campaign*		
GetDataInsights	Grants permission to get data insights from a data insights job	Read	dataInsightsJob*		
GetPersonalizedRanking	Grants permission to get a re-ranked list of recommendations	Read	campaign*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetRecommendations	Grants permission to get a list of recommendations from a campaign	Read	campaign*		
GetSolutionMetrics	Grants permission to get metrics for a solution version	Read	solution*		
ListBatchInferenceJobs	Grants permission to list batch inference jobs	List			
ListBatchSegmentJobs	Grants permission to list batch segment jobs	List			
ListCampaigns	Grants permission to list campaigns	List			
ListDataDeletionJobs	Grants permission to list data deletion jobs	List			
ListDataInsightsJobs	Grants permission to list data insights jobs	List			
ListDatasetExportJobs	Grants permission to list dataset export jobs	List			
ListDatasetGroups	Grants permission to list dataset groups	List			
ListDatasetImportJobs	Grants permission to list dataset import jobs	List			
ListDatasets	Grants permission to list datasets	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListEventTrackers	Grants permission to list event trackers	List			
ListFilters	Grants permission to list filters	List			
ListMetricAttributionMetrics	Grants permission to list metric attribution metrics	List			
ListMetricAttributions	Grants permission to list metric attributions	List			
ListRecipes	Grants permission to list recipes	List			
ListRecommenders	Grants permission to list recommenders	List			
ListSchemas	Grants permission to list schemas	List			
ListSolutionVersions	Grants permission to list versions of a solution	List			
ListSolutions	Grants permission to list solutions	List			
ListTagsForResource	Grants permission to list tags for a resource	List			
PutActionInteractions	Grants permission to put real time action interaction data	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutActions	Grants permission to ingest Actions data	Write	dataset*		
PutEvents	Grants permission to put real time event data	Write			
PutItems	Grants permission to ingest Items data	Write	dataset*		
PutUsers	Grants permission to ingest Users data	Write	dataset*		
StartRecommender	Grants permission to start a recommender	Write	recommender*		
StopRecommender	Grants permission to stop a recommender	Write	recommender*		
StopSolutionVersionCreation	Grants permission to stop a solution version creation	Write	solution*		
TagResource	Grants permission to tag a resource	Tagging			
UntagResource	Grants permission to untag a resource	Tagging			
UpdateCampaign	Grants permission to update a campaign	Write	campaign*		
UpdateDataset	Grants permission to update a dataset	Write	dataset*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateMetricAttribution	Grants permission to update a metric attribution	Write	metricAttribution*		
UpdateRecommender	Grants permission to update a recommender	Write	recommender*		
UpdateSolution	Grants permission to update a solution	Write	solution*		

Resource types defined by Amazon Personalize

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
schema	`arn:${Partition}:personalize:${Region}:${Account}:schema/${ResourceId}`	
featureTransformation	`arn:${Partition}:personalize:::feature-transformation/${ResourceId}`	
dataset	`arn:${Partition}:personalize:${Region}:${Account}:dataset/${ResourceId}`	
datasetGroup	`arn:${Partition}:personalize:${Region}:${Account}:dataset-group/${ResourceId}`	

Resource types	ARN	Condition keys
datasetImportJob	arn:${Partition}:personalize:${Region}:${Account}:dataset-import-job/${ResourceId}	
dataInsightsJob	arn:${Partition}:personalize:${Region}:${Account}:data-insights-job/${ResourceId}	
datasetExportJob	arn:${Partition}:personalize:${Region}:${Account}:dataset-export-job/${ResourceId}	
dataDeletionJob	arn:${Partition}:personalize:${Region}:${Account}:data-deletion-job/${ResourceId}	
solution	arn:${Partition}:personalize:${Region}:${Account}:solution/${ResourceId}	
campaign	arn:${Partition}:personalize:${Region}:${Account}:campaign/${ResourceId}	
eventTracker	arn:${Partition}:personalize:${Region}:${Account}:event-tracker/${ResourceId}	
recipe	arn:${Partition}:personalize:::recipe/${ResourceId}	
algorithm	arn:${Partition}:personalize:::algorithm/${ResourceId}	
batchInferenceJob	arn:${Partition}:personalize:${Region}:${Account}:batch-inference-job/${ResourceId}	

Resource types	ARN	Condition keys
filter	`arn:${Partition}:personalize:${Region}:${Account}:filter/${ResourceId}`	
recommender	`arn:${Partition}:personalize:${Region}:${Account}:recommender/${ResourceId}`	
batchSegmentJob	`arn:${Partition}:personalize:${Region}:${Account}:batch-segment-job/${ResourceId}`	
metricAttribution	`arn:${Partition}:personalize:${Region}:${Account}:metric-attribution/${ResourceId}`	

Condition keys for Amazon Personalize

Personalize 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 Amazon global condition context keys.

Actions, resources, and condition keys for Amazon Polly

Amazon Polly (service prefix: `polly`) 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 Polly

- Resource types defined by Amazon Polly
- Condition keys for Amazon Polly

Actions defined by Amazon Polly

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 Amazon. 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.

> **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
DeleteLexicon	Grants permission to delete the specified pronunciation lexicon stored in an Amazon Web Services Region	Write	lexicon*		
DescribeVoices	Grants permission to describe the list of voices that are available for use when requesting speech synthesis	List			
GetLexicon	Grants permission to retrieve the content of the specified pronunciation lexicon stored in an Amazon Web Services Region	Read	lexicon*		
GetSpeechSynthesisTask	Grants permission to get information about specific speech synthesis task	Read			
ListLexicons	Grants permission to list the pronunciation lexicons stored in an Amazon Web Services Region	List			
ListSpeechSynthesisTasks	Grants permission to list requested speech synthesis tasks	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutLexicon	Grants permission to store a pronunciation lexicon in an Amazon Web Services Region	Write	lexicon*		
StartSpeechSynthesisTask	Grants permission to synthesize long inputs to the provided S3 location	Write	lexicon		s3:PutObject
SynthesizeSpeech	Grants permission to synthesize speech	Read	lexicon		

Resource types defined by Amazon Polly

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
lexicon	`arn:${Partition}:polly:${Region}:${Account}:lexicon/${LexiconName}`	

Condition keys for Amazon Polly

Polly 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 Amazon global condition context keys.

Actions, resources, and condition keys for Amazon Price List

Amazon 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 Amazon Price List
- Resource types defined by Amazon Price List
- Condition keys for Amazon Price List

Actions defined by Amazon 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 Amazon. 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.

> **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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 Amazon Price List

Amazon Price List does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon Price List, specify `"Resource": "*"` in your policy.

Condition keys for Amazon 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 Amazon global condition context keys.

Actions, resources, and condition keys for Amazon Private Certificate Authority

Amazon 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 Amazon Private Certificate Authority
- Resource types defined by Amazon Private Certificate Authority
- Condition keys for Amazon Private Certificate Authority

Actions defined by Amazon 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 Amazon. 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.

> **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 Amazon 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 Amazon Private CA	Write	certificate-authority*		
CreatePermission	Grants permission to create a permission for an Amazon Private CA	Permissions management	certificate-authority*		
DeleteCertificateAuthority	Grants permission to delete an Amazon Private CA and its associated private key and configuration	Write	certificate-authority*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeletePermission	Grants permission to delete a permission for an Amazon Private CA	Permissions management	certificate-authority*		
DeletePolicy	Grants permission to delete the policy for an Amazon Private CA	Permissions management	certificate-authority*		
DescribeCertificateAuthority	Grants permission to return a list of the configuration and status fields contained in the specified Amazon Private CA	Read	certificate-authority*		
DescribeCertificateAuthorityAuditReport	Grants permission to return the status and information about an Amazon Private CA audit report	Read	certificate-authority*		
GetCertificate	Grants permission to retrieve an Amazon Private CA certificate and certificate chain for the certificate authority specified by an ARN	Read	certificate-authority*		
GetCertificateAuthorityCertificate	Grants permission to retrieve an Amazon Private CA certificate and certificate chain for the certificate authority specified by an ARN	Read	certificate-authority*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetCertificateAuthorityCsr	Grants permission to retrieve an Amazon Private CA certificate signing request (CSR) for the certificate-authority specified by an ARN	Read	certificate-authority*		
GetPolicy	Grants permission to retrieve the policy on an Amazon Private CA	Read	certificate-authority*		
ImportCertificateAuthorityCertificate	Grants permission to import an SSL/TLS certificate into Amazon Private CA for use as the CA certificate of an Amazon Private CA	Write	certificate-authority*		
IssueCertificate	Grants permission to issue an Amazon Private CA certificate	Write	certificate-authority*		
				acm-pca:TemplateArn	
ListCertificateAuthorities	Grants permission to retrieve a list of the Amazon Private CA certificate authority ARNs, and a summary of the status of each CA in the calling account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPermissions	Grants permission to list the permissions that have been applied to the Amazon Private CA certificate authority	Read	certificate-authority*		
ListTags	Grants permission to list the tags that have been applied to the Amazon Private CA certificate authority	Read	certificate-authority*		
PutPolicy	Grants permission to put a policy on an Amazon Private CA	Permissions management	certificate-authority*		
RestoreCertificateAuthority	Grants permission to restore an Amazon 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 Amazon Private CA	Write	certificate-authority*		
TagCertificateAuthority	Grants permission to add one or more tags to an Amazon Private CA	Tagging	certificate-authority*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagCertificateAuthority	Grants permission to remove one or more tags from an Amazon Private CA	Tagging	certificate-authority*	aws:RequestTag/${TagKey}	
				aws:TagKeys	
UpdateCertificateAuthority	Grants permission to update the configuration of an Amazon Private CA	Write	certificate-authority*		

Resource types defined by Amazon 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 Amazon Private Certificate Authority

Amazon 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 Amazon 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 Purchase Orders Console

Amazon Purchase Orders Console (service prefix: `purchase-orders`) 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 Purchase Orders Console
- Resource types defined by Amazon Purchase Orders Console
- Condition keys for Amazon Purchase Orders Console

Actions defined by Amazon Purchase Orders 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 Amazon. 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.

> **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
AddPurchaseOrder [permission only]	Grants permission to add a new purchase order	Write	purchase-order*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeletePurchaseOrder [permission only]	Grants permission to delete a purchase order	Write	purchase-order*		
				aws:ResourceTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey}	
GetConsoleActionSetEnforced [permission only]	Grants permission to view whether existing or fine-grained IAM actions are being used to control authorization to Billing, Cost Management, and Account consoles	Read			
GetPurchaseOrder [permission only]	Grants permission to get a purchase order	Read	purchase-order*		
				aws:ResourceTag/${TagKey}	
ListPurchaseOrderInvoices [permission only]	Grants permission to list purchase order invoices	List	purchase-order*		
				aws:ResourceTag/${TagKey}	
ListPurchaseOrders [permission only]	Grants permission to list all purchase orders for an account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource [permission only]	Grants permission to list tags for a purchase order	Read	purchase-order		
				aws:ResourceTag/${TagKey}	
ModifyPurchaseOrders [permission only]	Grants permission to modify purchase orders and details	Write	purchase-order*		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
TagResource [permission only]	Grants permission to tag purchase orders with given key value pairs	Tagging	purchase-order*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource [permission only]	Grants permission to remove tags from a purchase order	Tagging	purchase-order*		
				aws:TagKeys 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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdatePurchaseOrder [permission only]	Grants permission to update an existing purchase order	Write	purchase-order*		
				aws:ResourceTag/${TagKey}	
UpdatePurchaseOrderStatus [permission only]	Grants permission to set purchase order status	Write	purchase-order*		
				aws:ResourceTag/${TagKey}	
ViewPurchaseOrders [permission only]	Grants permission to view purchase orders and details	Read	purchase-order		
				aws:ResourceTag/${TagKey}	

Resource types defined by Amazon Purchase Orders Console

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
purchase-order	`arn:${Partition}:purchase-orders::${Account}:purchase-order/${ResourceName}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Purchase Orders Console

Amazon Purchase Orders Console 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 Amazon global condition context keys.

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

Actions, resources, and condition keys for Amazon QuickSight

Amazon QuickSight (service prefix: `quicksight`) 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 QuickSight
- Resource types defined by Amazon QuickSight
- Condition keys for Amazon QuickSight

Actions defined by Amazon QuickSight

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 Amazon. 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.

> **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
AccountConfigurations [permission only]	Grants permission to enable setting default access to Amazon resources	Write			
BatchCreateTopicReviewedAnswer	Grants permission to create reviewed answers for a topic	Write	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
BatchDeleteTopicReviewedAnswer	Grants permission to delete reviewed answers for a topic	Write	topic*		
				aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
CancelIngestion	Grants permission to cancel a SPICE ingestions on a dataset	Write	ingestion*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAccountCustomization	Grants permission to create an account customization for QuickSight account or namespace	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAccountSubscription	Grants permission to subscribe to QuickSight	Write		quicksight:Edition quicksight:DirectoryType	
CreateAdmin [permission only]	Grants permission to provision Amazon QuickSight administrators, authors, and readers	Write	user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAnalysis	Grants permission to create an analysis from a template	Write	analysis*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateBrand	Grants permission to create an Amazon QuickSight brand	Write	brand*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomPermissions	Grants permission to create a QuickSight custom permissions resource	Write	custompermissions*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDashboard	Grants permission to create a QuickSight Dashboard	Write	dashboard*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSet	Grants permission to create a dataset	Write	datasource*		quicksight:PassDataSource
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDataSource	Grants permission to create a data source	Write		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateEmailCustomizationTemplate [permission only]	Grants permission to create a QuickSight email customization template	Write	emailCustomizationTemplate*		
CreateFolder	Grants permission to create a QuickSight folder	Write	folder*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFolderMembership	Grants permission to add a QuickSight Dashboard, Analysis or Dataset to a QuickSight Folder	Write	folder*		
			analysis		
			dashboard		
			dataset		
CreateGroup	Grants permission to create a QuickSight group	Write	group*		
CreateGroupMembership	Grants permission to add a QuickSight user to a QuickSight group	Write	group*	quicksight:UserName	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateIAMPolicyAssignment	Grants permission to create an assignment with one specified IAM Policy ARN that will be assigned to specified groups or users of QuickSight	Write	assignment*		
CreateIngestion	Grants permission to start a SPICE ingestion on a dataset	Write	ingestion*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateNamespace	Grants permission to create an QuickSight namespace	Write	namespace*		ds:CreateIdentityPoolDirectory
CreateReader [permission only]	Grants permission to provision Amazon QuickSight readers	Write	user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRefreshSchedule	Grants permission to create a refresh schedule for a dataset	Write	refreshschedule*		
CreateRoleMembership	Grants permission to add a group member to a role	Write		quicksight:Group identitystore:GroupId	
CreateTemplate	Grants permission to create a template	Write	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTemplateAlias	Grants permission to create a template alias	Write	template*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTheme	Grants permission to create a theme	Write	theme*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateThemeAlias	Grants permission to create an alias for a theme version	Write	theme*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTopic	Grants permission to create a topic	Write	dataset*		quicksight:PassDataSet
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTopicRefreshSchedule	Grants permission to create a refresh schedule for a topic	Write	topic*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateUser [permission only]	Grants permission to provision Amazon QuickSight authors and readers	Write	user*		
CreateVPCConnection	Grants permission to create a vpc connection	Write		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
DeleteAccountCustomization	Grants permission to delete an account customization for QuickSight account or namespace	Write	customization*		
DeleteAccountSubscription	Grants permission to delete a QuickSight account	Write	account*		
DeleteAnalysis	Grants permission to delete an analysis	Write	analysis*		
DeleteBrand	Grants permission to delete an Amazon QuickSight brand	Write	brand*		
DeleteBrandAssignment	Grants permission to delete a brand assignment	Write			
DeleteCustomPermissions	Grants permission to delete a QuickSight custom permissions resource	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteDashboard	Grants permission to delete a QuickSight Dashboard	Write	dashboard*		
DeleteDataSet	Grants permission to delete a dataset	Write	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDataSetRefreshProperties	Grants permission to delete dataset refresh properties for a dataset	Write	dataset*		
DeleteDataSource	Grants permission to delete a data source	Write	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDefaultQBusinessApplication	Grants permission to delete linked QBusiness application for QuickSight account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteEmailCustomizationTemplate [permission only]	Grants permission to delete a QuickSight email customization template	Write	emailCustomizationTemplate*		
DeleteFolder	Grants permission to delete a QuickSight Folder	Write	folder*		
DeleteFolderMembership	Grants permission to remove a QuickSight Dashboard, Analysis or Dataset from a QuickSight Folder	Write	folder*		
			analysis		
			dashboard		
			dataset		
DeleteGroup	Grants permission to remove a user group from QuickSight	Write	group*		
DeleteGroupMembership	Grants permission to remove a user from a group so that he/she is no longer a member of the group	Write	group*	quicksight:UserName	
DeleteIAMPolicyAssignment	Grants permission to update an existing assignment	Write	assignment*		
DeleteIdentityPropagationConfig	Grants permission to remove Amazon services for trusted identity propagation in QuickSight	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteNamespace	Grants permission to delete a QuickSight namespace	Write	namespace*		ds:DeleteDirectory
DeleteRefreshSchedule	Grants permission to delete a refresh schedule for a dataset	Write	refreshschedule*		
DeleteRoleCustomPermission	Grants permission to remove the custom permission associated with a role	Write			
DeleteRoleMembership	Grants permission to remove a group member from a role	Write		quicksight:Group identitystore:GroupId	
DeleteTemplate	Grants permission to delete a template	Write	template*		
DeleteTemplateAlias	Grants permission to delete a template alias	Write	template*		
DeleteTheme	Grants permission to delete a theme	Write	theme*		
DeleteThemeAlias	Grants permission to delete the alias of a theme	Write	theme*		
DeleteTopic	Grants permission to delete a topic	Write	topic*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteTopicRefreshSchedule	Grants permission to delete a refresh schedule for a topic	Write	topic*		
DeleteUser	Grants permission to delete a QuickSight user, given the user name	Write	user*		
DeleteUserByPrincipalId	Grants permission to deletes a user identified by its principal ID	Write	user*		
DeleteUserCustomPermission	Grants permission to remove the custom permission associated with a user	Write	user*		
DeleteVPCConnection	Grants permission to delete a vpc connection	Write	vpcconnection*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeAccountCustomization	Grants permission to describe an account customization for QuickSight account or namespace	Read	customization*		
DescribeAccountSettings	Grants permission to describe the administrative account settings for QuickSight account	Read			
DescribeAccountSubscription	Grants permission to describe a QuickSight account	Read	account*		
DescribeAnalysis	Grants permission to describe an analysis	Read	analysis*		
DescribeAnalysisPermissions	Grants permission to describe permissions for an analysis	Read	analysis*		
DescribeAssetBundleExportJob	Grants permission to describe an asset bundle export job	Read	assetBundleExportJob*		
DescribeAssetBundleImportJob	Grants permission to describe an asset bundle import job	Read	assetBundleImportJob*		
DescribeBrand	Grants permission to describe a brand	Read	brand*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeBrandAssignment	Grants permission to describe a brand assignment	Read			
DescribeBrandPublishedVersion	Grants permission to describes the published version of the brand	Read	brand*		
DescribeCustomPermissions	Grants permission to describe a custom permissions resource in a QuickSight account	Read	custompermissions*		
DescribeDashboard	Grants permission to describe a QuickSight Dashboard	Read	dashboard*		
DescribeDashboardPermissions	Grants permission to describe permissions for a QuickSight Dashboard	Read	dashboard*		
DescribeDashboardSnapshotJob	Grants permission to describe a dashboard snapshot job	Read	dashboardSnapshotJob*		
DescribeDashboardSnapshotJobResult	Grants permission to describe result of a dashboard snapshot job	Read	dashboardSnapshotJob*		
DescribeDashboardsQAConfiguration	Grants permission to describe dashboards qa configuration	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDataSet	Grants permission to describe a dataset	Read	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeDataSetPermissions	Grants permission to describe the resource policy of a dataset	Permissions management	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeDataSetRefreshProperties	Grants permission to describe refresh properties for a dataset	Read	dataset*		
DescribeDataSource	Grants permission to describe a data source	Read	datasource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeDataSourcePermissions	Grants permission to describe the resource policy of a data source	Permissions management	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeDefaultQBusinessApplication	Grants permission to describe linked QBusiness application Id for QuickSight account	Read			
DescribeEmailCustomizationTemplate [permission only]	Grants permission to describe a QuickSight email customization template	Read	emailCustomizationTemplate*		
DescribeFolder	Grants permission to describe a QuickSight Folder	Read	folder*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeFolderPermissions	Grants permission to describe permissions for a QuickSight Folder	Read	folder*		
DescribeFolderResolvedPermissions	Grants permission to describe resolved permissions for a QuickSight Folder	Read	folder*		
DescribeGroup	Grants permission to describe a QuickSight group	Read	group*		
DescribeGroupMembership	Grants permission to describe a QuickSight group member	Read	group*	quicksight:UserName	
DescribeIAMPolicyAssignment	Grants permission to describe an existing assignment	Read	assignment*		
DescribeIngestion	Grants permission to describe a SPICE ingestion on a dataset	Read	ingestion*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeIpRestriction	Grants permission to describe the IP restrictions for QuickSight account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeKeyRegistration	Grants permission to describe QuickSight key registration	Read			
DescribeNamespace	Grants permission to describe a QuickSight namespace	Read	namespace*		
DescribeQPersonalizationConfiguration	Grants permission to describe a personalization configuration	Read			
DescribeQuickSightQSearchConfiguration	Grants permission to describe QuickSight Q Search configuration	Read			
DescribeRefreshSchedule	Grants permission to describe a refresh schedule for a dataset	Read	refreshschedule*		
DescribeRoleCustomPermission	Grants permission to describe the custom permission associated with a role	Read			
DescribeTemplate	Grants permission to describe a template	Read	template*		
DescribeTemplateAlias	Grants permission to describe a template alias	Read	template*		
DescribeTemplatePermissions	Grants permission to describe permissions for a template	Read	template*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeTheme	Grants permission to describe a theme	Read	theme*		
DescribeThemeAlias	Grants permission to describe a theme alias	Read	theme*		
DescribeThemePermissions	Grants permission to describe permissions for a theme	Read	theme*		
DescribeTopic	Grants permission to describe a topic	Read	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeTopicPermissions	Grants permission to describe the resource policy of a topic	Permissions management	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeTopicRefresh	Grants permission to describe the refresh status of a topic	Read	topic*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
DescribeTopicRefreshSchedule	Grants permission to describe a refresh schedule for a topic	Read	topic*		
DescribeUser	Grants permission to describe a QuickSight user given the user name	Read	user*		
DescribeVPCConnection	Grants permission to describe a vpc connection	Read	vpcconnection*		
				aws:RequestTag/${TagKey} aws:TagKeys	
GenerateEmbedUrlForAnonymousUser	Grants permission to generate a URL used to embed a QuickSight Dashboard or Q Topic for a user not registered with QuickSight	Write	namespace*		
			dashboard		
			theme		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			topic		
				aws:TagKeys aws:RequestTag/${TagKey} quicksight:AllowedEmbeddingDomains	
GenerateEmbedUrlForRegisteredUser	Grants permission to generate a URL used to embed a QuickSight Dashboard for a user registered with QuickSight	Write	user*		
				quicksight:AllowedEmbeddingDomains	
GenerateEmbedUrlForRegisteredUserWithIdentity	Grants permission to generate a URL used to embed a QuickSight Experience for a user registered with QuickSight using Identity-enhanced role session	Write		quicksight:AllowedEmbeddingDomains	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAnonymousUserEmbedUrl [permission only]	Grants permission to get a URL used to embed a QuickSight Dashboard for a user not registered with QuickSight	Read			
GetAuthCode [permission only]	Grants permission to get an auth code representing a QuickSight user	Read	user*		
GetDashboardEmbedUrl	Grants permission to get a URL used to embed a QuickSight Dashboard	Read	dashboard*		
GetGroupMapping [permission only]	Grants permission to use Amazon QuickSight, in Enterprise edition, to identify and display the Microsoft Active Directory (Microsoft Active Directory) directory groups that are mapped to roles in Amazon QuickSight	Read			
GetSessionEmbedUrl	Grants permission to get a URL to embed QuickSight console experience	Read			
ListAnalyses	Grants permission to list all analyses in an account	List	analysis*		
ListAssetBundleExportJobs	Grants permission to list all asset bundle export jobs	List	assetBundleExportJob*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAssetBundleImportJobs	Grants permission to list all asset bundle import jobs	List	assetBundleImportJob*		
ListBrands	Grants permission to lists all brands in an Amazon QuickSight account	List			
ListCustomPermissions	Grants permission to list custom permissions resources in QuickSight account	List			
ListCustomerManagedKeys [permission only]	Grants permission to list all registered customer managed keys	List			
ListDashboardVersions	Grants permission to list all versions of a QuickSight Dashboard	List	dashboard*		
ListDashboards	Grants permission to list all Dashboards in a QuickSight Account	List	dashboard*		
ListDataSets	Grants permission to list all datasets	List		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDataSources	Grants permission to list all data sources	List		aws:RequestTag/${TagKey} aws:TagKeys	
ListFolderMembers	Grants permission to list all members in a folder	Read	folder*		
ListFolders	Grants permission to list all Folders in a QuickSight Account	List	folder*		
ListFoldersForResource	Grants permission to list all Folders in which a QuickSight resource is a member	List	analysis		
			dashboard		
			dataset		
			datasource		
			topic		
ListGroupMemberships	Grants permission to list member users in a group	List	group*		
ListGroups	Grants permission to list all user groups in QuickSight	List	group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListIAMPolicyAssignments	Grants permission to list all assignments in the current Amazon QuickSight account	List	assignment*		
ListIAMPolicyAssignmentsForUser	Grants permission to list all assignments assigned to a user and the groups it belongs	List	assignment*		
ListIdentityPropagationConfigs	Grants permission to list Amazon services enabled for trusted identity propagation in QuickSight	List			
ListIngestions	Grants permission to list all SPICE ingestions on a dataset	List		aws:RequestTag/${TagKey} aws:TagKeys	
ListKMSKeysForUser [permission only]	Grants permission to list a user's KMS keys	List			
ListNamespaces	Grants permission to lists all namespaces in a QuickSight account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListRefreshSchedules	Grants permission to list all refresh schedules on a dataset	List			
ListRoleMemberships	Grants permission to list the members of a role	List			
ListTagsForResource	Grants permission to list tags of a QuickSight resource	Read	analysis		
			brand		
			customization		
			custompermissions		
			dashboard		
			dataset		
			datasource		
			folder		
			template		
			theme		
			topic		
			vpcconnection		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTemplateAliases	Grants permission to list all aliases for a template	List	template*		
ListTemplateVersions	Grants permission to list all versions of a template	List	template*		
ListTemplates	Grants permission to list all templates in a QuickSight account	List	template*		
ListThemeAliases	Grants permission to list all aliases of a theme	List	theme*		
ListThemeVersions	Grants permission to list all versions of a theme	List	theme*		
ListThemes	Grants permission to list all themes in an account	List	theme*		
ListTopicRefreshSchedules	Grants permission to list all refresh schedules on a topic	List			
ListTopicReviewedAnswers	Grants permission to list all reviewed answers for topic	List		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTopics	Grants permission to list all topics	List		aws:RequestTag/${TagKey} aws:TagKeys	
ListUserGroups	Grants permission to list groups that a given user is a member of	List	user*		
ListUsers	Grants permission to list all of the QuickSight users belonging to this account	List	user*		
ListVPCConnections	Grants permission to list all vpc connections	List		aws:RequestTag/${TagKey} aws:TagKeys	
PassDataSet [permission only]	Grants permission to use a dataset for a template	Read	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PassDataSource [permission only]	Grants permission to use a data source for a data set	Read	datasource*		
				aws:RequestTag/${TagKey} aws:TagKeys	
PredictQAResults	Grants permission to predict QA results	Read	dashboard		
			topic		
PutDataSetRefreshProperties	Grants permission to put dataset refresh properties for a dataset	Write	dataset*		
RegisterCustomerManagedKey [permission only]	Grants permission to register a customer managed key	Write			
RegisterUser	Grants permission to create a QuickSight user, whose identity is associated with the IAM identity/role specified in the request	Write	user*	quicksight:IamArn quicksight:SessionName	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RemoveCustomerManagedKey [permission only]	Grants permission to remove a customer managed key	Write			
RestoreAnalysis	Grants permission to restore a deleted analysis	Write	analysis*		
ScopeDownPolicy [permission only]	Grants permission to manage scoping policies for permissions to Amazon resources	Write			
SearchAnalyses	Grants permission to search for a sub-set of analyses	List	analysis*		
SearchDashboards	Grants permission to search for a sub-set of QuickSight Dashboards	List	dashboard*		
SearchDataSets	Grants permission to search for a sub-set of QuickSight DatSets	List	dataset*		
SearchDataSources	Grants permission to search for a sub-set of QuickSight Data Sources	List	datasource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SearchDirectoryGroups [permission only]	Grants permission to use Amazon QuickSight, in Enterprise edition, to display your Microsoft Active Directory directory groups so that you can choose which ones to map to roles in Amazon QuickSight	List			
SearchFolders	Grants permission to search for a sub-set of QuickSight Folders	Read	folder*		
SearchGroups	Grants permission to search for a sub-set of QuickSight groups	List	group*		
SearchTopics	Grants permission to search for a sub-set of topics	List	topic*		
SearchUsers [permission only]	Grants permission to search the QuickSight users belonging to this account	List	user*		
SetGroupMapping [permission only]	Grants permission to use Amazon QuickSight, in Enterprise edition, to display your Microsoft Active Directory directory groups so that you can choose which ones to map to roles in Amazon QuickSight	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartAssetBundleExportJob	Grants permission to start an asset bundle export job	Write	assetBundleExportJob*		
StartAssetBundleImportJob	Grants permission to start an asset bundle import job	Write	assetBundleImportJob*		
StartDashboardSnapshotJob	Grants permission to start a dashboard snapshot job	Write	dashboardSnapshotJob*		
StartDashboardSnapshotJobSchedule	Grants permission to start a dashboard snapshot job schedule	Write			
Subscribe [permission only]	Grants permission to subscribe to Amazon QuickSight, and also to allow the user to upgrade the subscription to Enterprise edition	Write		quicksight:Edition quicksight:DirectoryType	
TagResource	Grants permission to add tags to a QuickSight resource	Tagging	analysis		
			brand		
			customization		
			custompermissions		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			dashboard		
			dataset		
			datasource		
			folder		
			ingestion		
			template		
			theme		
			topic		
			vpcconnection		
				aws:TagKeys aws:RequestTag/${TagKey}	
Unsubscribe [permission only]	Grants permission to unsubscribe from Amazon QuickSight, which permanently deletes all users and their resources from Amazon QuickSight	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagResource	Grants permission to remove tags from a QuickSight resource	Tagging	analysis		
			brand		
			customization		
			custompermissions		
			dashboard		
			dataset		
			datasource		
			folder		
			ingestion		
			template		
			theme		
			topic		
			vpcconnection		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAccountCustomization	Grants permission to update an account customization for QuickSight account or namespace	Write	customization*		
UpdateAccountSettings	Grants permission to update the administrative account settings for QuickSight account	Write			
UpdateAnalysis	Grants permission to update an analysis	Write	analysis*		
UpdateAnalysisPermissions	Grants permission to update permissions for an analysis	Permissions management	analysis*		
UpdateApplicationWithTokenExchangeGrant	Grants permission to update QuickSight IAM Identity Center application with Token Exchange grant	Write			
UpdateBrand	Grants permission to update a brand	Write	brand*		
UpdateBrandAssignment	Grants permission to update a brand assignment	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateBrandPublishedVersion	Grants permission to update the published version of a brand	Write	brand*		
UpdateCustomPermissions	Grants permission to update a QuickSight custom permissions resource	Write	custompermissions*		
UpdateDashboard	Grants permission to update a QuickSight Dashboard	Write	dashboard*		
UpdateDashboardLinks	Grants permission to update a QuickSight Dashboard's links	Write	dashboard*		
UpdateDashboardPermissions	Grants permission to update permissions for a QuickSight Dashboard	Permissions management	dashboard*		
UpdateDashboardPublishedVersion	Grants permission to update a QuickSight Dashboard's Published Version	Write	dashboard*		
UpdateDashboardsQAConfiguration	Grants permission to update dashboards qa configuration	Write			
UpdateDataSet	Grants permission to update a dataset	Write	dataset*		quicksight:PassDataSource
			datasource		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateDataSetPermissions	Grants permission to update the resource policy of a dataset	Permissions management	dataset*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateDataSource	Grants permission to update a data source	Write	datasource*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateDataSourcePermissions	Grants permission to update the resource policy of a data source	Permissions management	datasource*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateDefaultQBusinessApplication	Grants permission to update linked QBusiness application Id for QuickSight account	Write			
UpdateEmailCustomizationTemplate [permission only]	Grants permission to update a QuickSight email customization template	Write	emailCustomizationTemplate*		
UpdateFolder	Grants permission to update a QuickSight Folder	Write	folder*		
UpdateFolderPermissions	Grants permission to update permissions for a QuickSight Folder	Permissions management	folder*		
UpdateGroup	Grants permission to change group description	Write	group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateIAMPolicyAssignment	Grants permission to update an existing assignment	Write	assignment*		
UpdateIdentityPropagationConfig	Grants permission to add and update Amazon services for trusted identity propagation in QuickSight	Write			
UpdateIpRestriction	Grants permission to update the IP restrictions for QuickSight account	Write			
UpdateKeyRegistration	Grants permission to update QuickSight key registration	Write			
UpdatePublicSharingSettings	Grants permission to enable or disable public sharing on an account	Write			
UpdateQPersonalizationConfiguration	Grants permission to update a personalization configuration	Write			
UpdateQuickSightQSearchConfiguration	Grants permission to update QuickSight Q Search configuration	Write			
UpdateRefreshSchedule	Grants permission to update a refresh schedule for a dataset	Write	refreshschedule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateResourcePermissions [permission only]	Grants permission to update resource-level permissions in QuickSight	Write			
UpdateRoleCustomPermission	Grants permission to update the custom permission associated with a role	Write			
UpdateSPICECapacityConfiguration	Grants permission to update QuickSight SPICE capacity configuration	Write			
UpdateTemplate	Grants permission to update a template	Write	template*		
UpdateTemplateAlias	Grants permission to update a template alias	Write	template*		
UpdateTemplatePermissions	Grants permission to update permissions for a template	Permissions management	template*		
UpdateTheme	Grants permission to update a theme	Write	theme*		
UpdateThemeAlias	Grants permission to update the alias of a theme	Write	theme*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateThemePermissions	Grants permission to update permissions for a theme	Permissions management	theme*		
UpdateTopic	Grants permission to update a topic	Write	topic*		quicksight:PassDataSet
			dataset		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateTopicPermissions	Grants permission to update the resource policy of a topic	Permissions management	topic*		
				aws:RequestTag/${TagKey} aws:TagKeys	
UpdateTopicRefreshSchedule	Grants permission to update a refresh schedule for a topic	Write	topic*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateUser	Grants permission to update an Amazon QuickSight user	Write	user*		
UpdateUserCustomPermission	Grants permission to update the custom permission associated with a user	Write	user*		
UpdateVPCConnection	Grants permission to update a vpc connection	Write	vpcconnection*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	

Resource types defined by Amazon QuickSight

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:${Partition}:quicksight:${Region}:${Account}:account/${ResourceId}`	

Resource types	ARN	Condition keys
user	arn:${Partition}:quicksight:${Region}:${Account}:user/${ResourceId}	
group	arn:${Partition}:quicksight:${Region}:${Account}:group/${ResourceId}	
analysis	arn:${Partition}:quicksight:${Region}:${Account}:analysis/${ResourceId}	aws:ResourceTag/${TagKey}
dashboard	arn:${Partition}:quicksight:${Region}:${Account}:dashboard/${ResourceId}	aws:ResourceTag/${TagKey}
template	arn:${Partition}:quicksight:${Region}:${Account}:template/${ResourceId}	aws:ResourceTag/${TagKey}
vpcconnection	arn:${Partition}:quicksight:${Region}:${Account}:vpcConnection/${ResourceId}	aws:ResourceTag/${TagKey}
assetBundleExportJob	arn:${Partition}:quicksight:${Region}:${Account}:asset-bundle-export-job/${ResourceId}	
assetBundleImportJob	arn:${Partition}:quicksight:${Region}:${Account}:asset-bundle-import-job/${ResourceId}	
datasource	arn:${Partition}:quicksight:${Region}:${Account}:datasource/${ResourceId}	aws:ResourceTag/${TagKey}
dataset	arn:${Partition}:quicksight:${Region}:${Account}:dataset/${ResourceId}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
ingestion	arn:${Partition}:quicksight:${Region}:${Account}:dataset/${DatasetId}/ingestion/${ResourceId}	aws:ResourceTag/${TagKey}
refreshschedule	arn:${Partition}:quicksight:${Region}:${Account}:dataset/${DatasetId}/refresh-schedule/${ResourceId}	
theme	arn:${Partition}:quicksight:${Region}:${Account}:theme/${ResourceId}	aws:ResourceTag/${TagKey}
assignment	arn:${Partition}:quicksight::${Account}:assignment/${ResourceId}	
customization	arn:${Partition}:quicksight:${Region}:${Account}:customization/${ResourceId}	aws:ResourceTag/${TagKey}
namespace	arn:${Partition}:quicksight:${Region}:${Account}:namespace/${ResourceId}	
folder	arn:${Partition}:quicksight:${Region}:${Account}:folder/${ResourceId}	aws:ResourceTag/${TagKey}
emailCustomizationTemplate	arn:${Partition}:quicksight:${Region}:${Account}:email-customization-template/${ResourceId}	
topic	arn:${Partition}:quicksight:${Region}:${Account}:topic/${ResourceId}	aws:ResourceTag/${TagKey}
dashboardSnapshotJob	arn:${Partition}:quicksight:${Region}:${Account}:dashboard/${DashboardId}/snapshot-job/${ResourceId}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
brand	`arn:${Partition}:quicksight:${Region}:${Account}:brand/${ResourceId}`	aws:ResourceTag/${TagKey}
custompermissions	`arn:${Partition}:quicksight:${Region}:${Account}:custompermissions/${ResourceId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon QuickSight

Amazon QuickSight 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 Amazon global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by tag key-value pairs in the request	String
aws:ResourceTag/${TagKey}	Filters access by tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by tag keys	ArrayOfString
identitystore:GroupId	Filters access by IdentityStore group ARN	ARN
quicksight:AllowedEmbeddingDomains	Filters access by the allowed embedding domains	ArrayOfString

Condition keys	Description	Type
quicksight:DirectoryType	Filters access by the user management options	String
quicksight:Edition	Filters access by the edition of QuickSight	String
quicksight:Group	Filters access by QuickSight group ARN	ARN
quicksight:IamArn	Filters access by IAM user or role ARN	ARN
quicksight:KmsKeyArns	Filters access by KMS key ARNs	ArrayOfARN
quicksight:SessionName	Filters access by session name	String
quicksight:UserName	Filters access by user name	String

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 Amazon. 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.

> **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 Amazon 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	cev		
			cluster		
			cluster-endpoint		
			cluster-pg		
			cluster-snapshot		
			db		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			deployment		
			es		
			integration		
			og		
			pg		
			proxy		
			proxy-endpoint		
			ri		
			secgrp		
			shardgrp		
			snapshot		
			snapshot-tenant-database		
			subgrp		
			target-group		

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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
				aws:RequestTag/${TagKey} aws:TagKeys	
CopyDBClusterSnapshot	Grants permission to create a snapshot of a DB cluster	Write	cluster-snapshot*		rds:AddTagsToResource
				aws:RequestTag/${TagKey} aws:TagKeys	
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/${TagKey} aws:TagKeys	
CopyDBSnapshot	Grants permission to copy the specified DB snapshot	Write	snapshot*		rds:AddTagsToResource rds:CopyCustomDBEngineVersion
				aws:RequestTag/${TagKey} aws:TagKeys rds:CopyOptionGroup	
CopyOptionGroup	Grants permission to copy the specified option group	Write	og*		rds:AddTagsToResource

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

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

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	
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	

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}	
CreateDBParameterGroup	Grants permission to create a new 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}	
CreateDBProxy	Grants permission to create a database proxy	Write		aws:RequestTag/${TagKey} aws:TagKeys	iam:PassRole
CreateDBProxyEndpoint	Grants permission to create a database proxy endpoint	Write	proxy*		
			proxy-endpoint*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDBSnapshot	Grants permission to create a DBSnapshot	Write	db*		rds:AddTagsToResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			snapshot*		
				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*		
			global-cluster*		
CreateIntegration	Grants permission to create an Aurora zero-ETL integration with Redshift	Write	cluster*		kms:CreateGrant kms:DescribeKey rds:AddTagsToResource

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			integration*		
				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}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTenantDatabase	Grants permission to create a new tenant database	Write	db*		rds:AddTagsToResource
			tenant-database*		
				aws:RequestTag/${TagKey} aws:TagKeys rds:TenantDatabaseName	
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 Amazon Web Services 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 DBClusterParameterGroup 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*		
DescribeDBParameterGroups	Grants permission to return a list of DBParameterGroup descriptions	List	pg		
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		

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeReservedDBInstancesOfferings	Grants permission to list available reserved DB instance offerings	List			
DescribeSourceRegions	Grants permission to return a list of the source Amazon Web Services Regions where the current Amazon Web Services 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*		
DisableHttpEndpoint	Grants permission to disable http endpoint for a DB cluster	Write	cluster*		
DownloadCompleteDBLogFile	Grants permission to download specified log file	Read	db*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	cev		
			cluster		
			cluster-endpoint		
			cluster-pg		
			cluster-snapshot		
			db		
			es		
			integration		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			og		
			pg		
			proxy		
			proxy-endpoint		
			ri		
			secgrp		
			shardgrp		
			snapshot		
			snapshot-tenant-database		
			subgrp		
			target-group		
			tenant-database		
ModifyActivityStream	Grants permission to modify a database activity stream	Write	db*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	
PromoteReadReplica	Grants permission to promote a Read Replica DB instance to a standalone DB instance	Write	db*		
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*		
				aws:RequestTag/${TagKey} aws:TagKeys	
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*		
RemoveFromGlobalCluster	Grants permission to detach an Aurora secondary cluster from an Aurora global database cluster or DocumentDB global cluster	Write	cluster*		
			global-cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RemoveRoleFromDBCluster	Grants permission to disassociate an Amazon Identity and Access Management (IAM) role from an Amazon Aurora DB cluster	Write	cluster*		iam:PassRole
RemoveRoleFromDBInstance	Grants permission to disassociate an Amazon 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	cev		
			cluster		
			cluster-endpoint		
			cluster-pg		
			cluster-snapshot		
			db		
			deployment		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			es		
			integration		
			og		
			pg		
			proxy		
			proxy-endpoint		
			ri		
			secgrp		
			shardgrp		
			snapshot		
			snapshot-tenant-database		
			subgrp		
			target-group		
			tenant-database		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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*		
ResetDBParameterGroup	Grants permission to modify the parameters of a DB parameter group to the engine/system default value	Write	pg*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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
			cluster-pg*		
			og*		
			subgrp*		

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: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}	

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	
RestoreDBInstanceToPointInTime	Grants permission to restore a DB instance to an arbitrary point in time	Write	db*		iam:PassRole rds:AddTagsToResource rds:CreateTenantDatabase
			og*		
			pg*		
			subgrp*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			auto-backup		
				rds:BackupTarget aws:RequestTag/${TagKey} aws:TagKeys rds:req-tag/${TagKey}	
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartDBInstanceAutomatedBackupsReplication	Grants permission to start replication of automated backups to a different Amazon Web Services Region	Write	auto-backup*		
			db*		
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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopDBInstanceAutomatedBackupsReplication	Grants permission to stop automated backup replication for a DB instance	Write	db*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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:${DbClusterAutomatedBackupId}`	
auto-backup	`arn:${Partition}:rds:${Region}:${Account}:auto-backup:${DbInstanceAutomatedBackupId}`	

Resource types	ARN	Condition keys
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/${TagKey}
cluster-snapshot	`arn:${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}

Resource types	ARN	Condition keys
es	arn:${Partition}:rds:${Region}:${Account}:es:${SubscriptionName}	aws:ResourceTag/${TagKey} rds:es-tag/${TagKey}
global-cluster	arn:${Partition}:rds::${Account}:global-cluster:${GlobalCluster}	
og	arn:${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}

Resource types	ARN	Condition keys
snapshot	arn:${Partition}:rds:${Region}:${Account}:snapshot:${SnapshotName}	aws:ResourceTag/${TagKey} rds:snapshot-tag/${TagKey}
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 Amazon 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

Condition keys	Description	Type
rds:ManageMasterUserPassword	Filters access by the value that specifies whether RDS manages master user password in Amazon Secrets Manager for the DB instance or cluster	Bool
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: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 subscript ion	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 Amazon RDS IAM Authentication

Amazon RDS IAM Authentication (service prefix: `rds-db`) 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 IAM Authentication
- Resource types defined by Amazon RDS IAM Authentication
- Condition keys for Amazon RDS IAM Authentication

Actions defined by Amazon RDS IAM Authentication

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 Amazon. 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.

> **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
connect	Allows IAM role or user to connect to RDS database	Permissions management	db-user*		

Resource types defined by Amazon RDS IAM Authentication

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
db-user	`arn:${Partition}:rds-db:${Region}:${Account}:dbuser:${DbiResourceId}/${DbUserName}`	

Condition keys for Amazon RDS IAM Authentication

RDS IAM Authentication 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 Amazon global condition context keys.

Actions, resources, and condition keys for Amazon Recycle Bin

Amazon Recycle Bin (service prefix: `rbin`) 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 Recycle Bin
- Resource types defined by Amazon Recycle Bin
- Condition keys for Amazon Recycle Bin

Actions defined by Amazon Recycle Bin

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 Amazon. 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.

> **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
CreateRule	Grants permission to create a Recycle Bin retention rule	Write	rule*		
				aws:RequestTag/${TagKey} aws:TagKeys rbin:Request/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ResourceType	
DeleteRule	Grants permission to delete a Recycle Bin retention rule	Write	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	
GetRule	Grants permission to get detailed information about a Recycle Bin retention rule	Read	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	
ListRules	Grants permission to list the Recycle Bin retention rules in the Region	Read		rbin:Request/ResourceType	
ListTagsForResource		Read	rule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to list the tags associated with a resource			aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	
LockRule	Grants permission to lock an existing Recycle Bin retention rule	Write	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	
TagResource	Grants permission to add or update tags of a resource	Tagging	rule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys rbin:Attribute/ResourceType	
UnlockRule	Grants permission to unlock an existing Recycle Bin retention rule	Write	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	
UntagResource	Grants permission to remove tags associated with a resource	Tagging	rule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:TagKeys rbin:Attribute/ResourceType	
UpdateRule	Grants permission to update an existing Recycle Bin retention rule	Write	rule*		
				aws:ResourceTag/${TagKey} rbin:Attribute/ResourceType	

Resource types defined by Amazon Recycle Bin

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
rule	`arn:${Partition}:rbin:${Region}:${Account}:rule/${ResourceName}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Recycle Bin

Amazon Recycle Bin 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 Amazon global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by a tag's key and value in a request	String
aws:ResourceTag/${TagKey}	Filters access by the presence of tag key-value pairs in the request	String
aws:TagKeys	Filters access by the tag keys in a request	ArrayOfString
rbin:Attribute/ResourceType	Filters access by the resource type of the existing rule	String
rbin:Request/ResourceType	Filters access by the resource type in a request	String

Actions, resources, and condition keys for Amazon Redshift

Amazon Redshift (service prefix: `redshift`) 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 Redshift
- Resource types defined by Amazon Redshift
- Condition keys for Amazon Redshift

Actions defined by Amazon Redshift

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 Amazon. 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.

> **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
AcceptReservedNodeExchange	Grants permission to exchange a DC1 reserved node for a DC2 reserved node with no changes to the configuration	Write			
AddPartner	Grants permission to add a partner integration to a cluster	Write			
AssociateDataShareConsumer	Grants permission to associate a consumer to a datashare	Write	datashare*		
				redshift:ConsumerArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				redshift:AllowWrites	
AuthorizeClusterSecurityGroupIngress	Grants permission to add an inbound (ingress) rule to an Amazon Redshift security group	Write	securitygroup*		
			securitygroupingress-ec2securitygroup*		
AuthorizeDataShare	Grants permission to authorize the specified datashare consumer to consume a datashare	Permissions management	datashare*		
				redshift:ConsumerIdentifier redshift:AllowWrites	
AuthorizeEndpointAccess	Grants permission to authorize endpoint related activities for redshift-managed vpc endpoint	Permissions management			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AuthorizeInboundIntegration [permission only]	Grants permission to Amazon Redshift to continuously validate that the target data warehouse can receive data replicated from the source ARN	Write	integration*		
AuthorizeSnapshotAccess	Grants permission to the specified Amazon Web Services account to restore a snapshot	Permissions management	snapshot*		
BatchDeleteClusterSnapshots	Grants permission to delete snapshots in a batch of size upto 100	Write	snapshot*		
BatchModifyClusterSnapshots	Grants permission to modify settings for a list of snapshots	Write	snapshot*		
CancelQuery [permission only]	Grants permission to cancel a query through the Amazon Redshift console	Write			
CancelQuerySession [permission only]	Grants permission to see queries in the Amazon Redshift console	Write			
CancelResize	Grants permission to cancel a resize operation	Write	cluster*		
CopyClusterSnapshot	Grants permission to copy a cluster snapshot	Write	snapshot*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAuthenticationProfile	Grants permission to create an Amazon Redshift authentication profile	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCluster	Grants permission to create a cluster	Write	cluster*		kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:GetRandomPassword

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterParameterGroup	Grants permission to create an Amazon Redshift parameter group	Write	parameergroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterSecurityGroup	Grants permission to create an Amazon Redshift security group	Write	securitygroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterSnapshot	Grants permission to create a manual snapshot of the specified cluster	Write	snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterSubnetGroup	Grants permission to create an Amazon Redshift subnet group	Write	subnetgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateClusterUser	Grants permission to automatically create the specified Amazon Redshift user if it does not exist	Permissions management	dbuser*		
				redshift:DbUser	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCustomDomainAssociation	Grants permission to create a custom domain name for a cluster	Write	cluster*		acm:DescribeCertificate
CreateEndpointAccess	Grants permission to create a redshift-managed vpc endpoint	Write			
CreateEventSubscription	Grants permission to create an Amazon Redshift event notification subscription	Write	eventsubscription*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateHsmClientCertificate	Grants permission to create an HSM client certificate that a cluster uses to connect to an HSM	Write	hsmclientcertificate*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateHsmConfiguration	Grants permission to create an HSM configuration that contains information required by a cluster to store and use database encryption keys in a hardware security module (HSM)	Write	hsmconfiguration*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateInboundIntegration [permission only]	Grants permission to the source principal to create an inbound integration for data to be replicated from the source into the target data warehouse	Write			
CreateIntegration	Grants permission to create an Amazon Redshift zero-ETL integration	Write	integration*		kms:CreateGrant kms:DescribeKey

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys redshift:IntegrationSourceArn redshift:IntegrationTargetArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateQev2IdcApplication [permission only]	Grants permission to create a qev2 idc application	Write			sso:CreateApplication sso:PutApplicationAccessScope sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateRedshiftIdcApplication	Grants permission to create a redshift idc application	Write			sso:CreateApplication sso:PutApplicationAccessScope sso:PutApplicationAuthenticationMethod sso:PutApplicationGrant
CreateSavedQuery [permission only]	Grants permission to create saved SQL queries through the Amazon Redshift console	Write			
CreateScheduledAction	Grants permission to create an Amazon Redshift scheduled action	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSnapshotCopyGrant	Grants permission to create a snapshot copy grant and encrypt copied snapshots in a destination Amazon Web Services Region	Permissions management	snapshotcopygrant*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshotSchedule	Grants permission to create a snapshot schedule	Write	snapshotschedule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateTags	Grants permission to add one or more tags to a specified resource	Tagging	cluster		
			eventsubscription		
			hsmclientcertificate		
			hsmconfiguration		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			integration		
			parametergroup		
			securitygroup		
			securitygroupingress-cidr		
			securitygroupingress-ec2securitygroup		
			snapshot		
			snapshotcopygrant		
			snapshotschedule		
			subnetgroup		
			usagelimit		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateUsageLimit	Grants permission to create a usage limit	Write	usagelimit*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeauthorizeDataShare	Grants permission to remove permission from the specified datashare consumer to consume a datashare	Permissions management	datashare*		
				redshift:ConsumerIdentifier	
DeleteAuthenticationProfile	Grants permission to delete an Amazon Redshift authentication profile	Write			
DeleteCluster	Grants permission to delete a previously provisioned cluster	Write	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteClusterParameterGroup	Grants permission to delete an Amazon Redshift parameter group	Write	parametergroup*		
DeleteClusterSecurityGroup	Grants permission to delete an Amazon Redshift security group	Write	securitygroup*		
DeleteClusterSnapshot	Grants permission to delete a manual snapshot	Write	snapshot*		
DeleteClusterSubnetGroup	Grants permission to delete a cluster subnet group	Write	subnetgroup*		
DeleteCustomDomainAssociation	Grants permission to delete a custom domain name for a cluster	Write	cluster*		
DeleteEndpointAccess	Grants permission to delete a redshift-managed vpc endpoint	Write			
DeleteEventSubscription	Grants permission to delete an Amazon Redshift event notification subscription	Write	eventsubscription*		
DeleteHsmClientCertificate	Grants permission to delete an HSM client certificate	Write	hsmclientcertificate*		
DeleteHsmConfiguration	Grants permission to delete an Amazon Redshift HSM configuration	Write	hsmconfiguration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteIntegration	Grants permission to delete an Amazon Redshift zero-ETL integration	Write	integration*		
				aws:ResourceTag/${TagKey}	
DeletePartner	Grants permission to delete a partner integration from a cluster	Write			
DeleteQev2IdcApplication [permission only]	Grants permission to delete a qev2 idc application	Write	qev2idcapplication*		sso:DeleteApplication
DeleteRedshiftIdcApplication	Grants permission to delete a redshift idc application	Write	redshiftidcapplication*		sso:DeleteApplication
DeleteResourcePolicy	Grants permission to delete the resource policy for a specified resource	Permissions management	namespace*		
DeleteSavedQueries [permission only]	Grants permission to delete saved SQL queries through the Amazon Redshift console	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteScheduledAction	Grants permission to delete an Amazon Redshift scheduled action	Write			
DeleteSnapshotCopyGrant	Grants permission to delete a snapshot copy grant	Write	snapshotcopygrant*		
DeleteSnapshotSchedule	Grants permission to delete a snapshot schedule	Write	snapshotschedule*		
DeleteTags	Grants permission to delete a tag or tags from a resource	Tagging	cluster		
			eventsubscription		
			hsmclientcertificate		
			hsmconfiguration		
			integration		
			parametergroup		
			securitygroup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			securitygroupingress-cidr		
			securitygroupingress-ec2securitygroup		
			snapshot		
			snapshotcopygrant		
			snapshotschedule		
			subnetgroup		
			usagelimit		
				aws:TagKeys	
DeleteUsageLimit	Grants permission to delete a usage limit	Write	usagelimit*		
DeregisterNamespace	Grants permission to deregister the specified namespace from a consumer	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeAccountAttributes	Grants permission to describe attributes attached to the specified Amazon Web Services account	Read			
DescribeAuthenticationProfiles	Grants permission to describe created Amazon Redshift authentication profiles	Read			
DescribeClusterDbRevisions	Grants permission to describe database revisions for a cluster	List			
DescribeClusterParameterGroups	Grants permission to describe Amazon Redshift parameter groups, including parameter groups you created and the default parameter group	Read			
DescribeClusterParameters	Grants permission to describe parameters contained within an Amazon Redshift parameter group	Read	parameter group*		
DescribeClusterSecurityGroups	Grants permission to describe Amazon Redshift security groups	Read			
DescribeClusterSnapshots	Grants permission to describe one or more snapshot objects, which contain metadata about your cluster snapshots	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeClusterSubnetGroups	Grants permission to describe one or more cluster subnet group objects, which contain metadata about your cluster subnet groups	Read			
DescribeClusterTracks	Grants permission to describe available maintenance tracks	List			
DescribeClusterVersions	Grants permission to describe available Amazon Redshift cluster versions	Read			
DescribeClusters	Grants permission to describe properties of provisioned clusters	List			
DescribeCustomDomainAssociations	Grants permission to describe custom domain names for a cluster	List			
DescribeDataShares	Grants permission to describe datashares created and consumed by your clusters	Read			
DescribeDataShares ForConsumer	Grants permission to describe only datashares consumed by your clusters	Read			
DescribeDataShares ForProducer	Grants permission to describe only datashares created by your clusters	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeDefaultClusterParameters	Grants permission to describe parameter settings for a parameter group family	Read			
DescribeEndpointAccess	Grants permission to describe redshift-managed vpc endpoints	Read			
DescribeEndpointAuthorization	Grants permission to authorize describe activity for redshift-managed vpc endpoint	List			
DescribeEventCategories	Grants permission to describe event categories for all event source types, or for a specified source type	Read			
DescribeEventSubscriptions	Grants permission to describe Amazon Redshift event notification subscriptions for the specified Amazon Web Services account	Read			
DescribeEvents	Grants permission to describe events related to clusters, security groups, snapshots, and parameter groups for the past 14 days	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeHsmClientCertificates	Grants permission to describe HSM client certificates	Read			
DescribeHsmConfigurations	Grants permission to describe Amazon Redshift HSM configurations	Read			
DescribeInboundIntegrations	Grants permission to list the inbound integrations	List		redshift:InboundIntegrationArn	
DescribeIntegrations	Grants permission to describe an Amazon Redshift zero-ETL integration	List	integration*		
				aws:ResourceTag/${TagKey}	
DescribeLoggingStatus	Grants permission to describe whether information, such as queries and connection attempts, is being logged for a cluster	Read	cluster*		
DescribeNodeConfigurationOptions	Grants permission to describe properties of possible node configurations such as node type, number of nodes, and disk usage for the specified action type	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeOrderableClusterOptions	Grants permission to describe orderable cluster options	Read			
DescribePartners	Grants permission to retrieve information about the partner integrations defined for a cluster	Read			
DescribeQev2IdcApplications [permission only]	Grants permission to describe qev2 idc applications	List			
DescribeQuery [permission only]	Grants permission to describe a query through the Amazon Redshift console	Read			
DescribeRedshiftIdcApplications	Grants permission to describe redshift idc applications	List			sso:GetApplicationGrant sso:ListApplicationAccessScopes

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeReservedNodeExchangeStatus	Grants permission to describe exchange status details and associated metadata for a reserved-node exchange. Statuses include such values as in progress and requested	Read			
DescribeReservedNodeOfferings	Grants permission to describe available reserved node offerings by Amazon Redshift	Read			
DescribeReservedNodes	Grants permission to describe the reserved nodes	Read			
DescribeResize	Grants permission to describe the last resize operation for a cluster	Read	cluster*		
DescribeSavedQueries [permission only]	Grants permission to describe saved queries through the Amazon Redshift console	Read			
DescribeScheduledActions	Grants permission to describe created Amazon Redshift scheduled actions	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeSnapshotCopyGrants	Grants permission to describe snapshot copy grants owned by the specified Amazon Web Services account in the destination Amazon Web Services Region	Read			
DescribeSnapshotSchedules	Grants permission to describe snapshot schedules	Read	snapshotschedule*		
DescribeStorage	Grants permission to describe account level backups storage size and provisional storage	Read			
DescribeTable [permission only]	Grants permission to describe a table through the Amazon Redshift console	Read			
DescribeTableRestoreStatus	Grants permission to describe status of one or more table restore requests made using the RestoreTableFromClusterSnapshot API action	Read			
DescribeTags	Grants permission to describe tags	Read	cluster		
			eventsubscription		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			hsmclientcertificate		
			hsmconfiguration		
			integration		
			parametergroup		
			securitygroup		
			securitygroupingress-cidr		
			securitygroupingress-ec2securitygroup		
			snapshot		
			snapshotcopygrant		
			snapshotschedule		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			subnetgroup		
			usagelimit		
DescribeUsageLimits	Grants permission to describe usage limits	Read	usagelimit*		
DisableLogging	Grants permission to disable logging information, such as queries and connection attempts, for a cluster	Write	cluster*		
DisableSnapshotCopy	Grants permission to disable the automatic copy of snapshots for a cluster	Write	cluster*		
DisassociateDataShareConsumer	Grants permission to disassociate a consumer from a datashare	Write	datashare*		
				redshift:ConsumerArn	
EnableLogging	Grants permission to enable logging information, such as queries and connection attempts, for a cluster	Write	cluster*		
EnableSnapshotCopy	Grants permission to enable the automatic copy of snapshots for a cluster	Write	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ExecuteQuery [permission only]	Grants permission to execute a query through the Amazon Redshift console	Write			
FailoverPrimaryCompute	Grants permission to failover the primary compute of an Multi-AZ cluster to another AZ	Write	cluster*		
FetchResults [permission only]	Grants permission to fetch query results through the Amazon Redshift console	Read			
GetClusterCredentials	Grants permission to get temporary credentials to access an Amazon Redshift database by the specified Amazon Web Services account	Write	dbuser*		
			dbgroup		
			dbname		
				redshift:DbName redshift:DbUser redshift:DurationSeconds	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetClusterCredentialsWithIAM	Grants permission to get enhanced temporary credentials to access an Amazon Redshift database by the specified Amazon Web Services account	Write	dbname		
				redshift:DbName redshift:DurationSeconds	
GetReservedNodeExchangeConfigurationOptions	Grants permission to get the configuration options for the reserved-node exchange	Read			
GetReservedNodeExchangeOfferings	Grants permission to get an array of DC2 ReservedNodeOfferings that matches the payment type, term, and usage price of the given DC1 reserved node	Read			
GetResourcePolicy	Grants permission to get the resource policy for a specified resource	Read	namespace*		
JoinGroup	Grants permission to join the specified Amazon Redshift group	Permissions management	dbgroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDatabases [permission only]	Grants permission to list databases through the Amazon Redshift console	List			
ListRecommendations	Grants permission to list Advisor recommendations	List			
ListSavedQueries [permission only]	Grants permission to list saved queries through the Amazon Redshift console	List			
ListSchemas [permission only]	Grants permission to list schemas through the Amazon Redshift console	List			
ListTables [permission only]	Grants permission to list tables through the Amazon Redshift console	List			
ModifyAquaConfiguration	Grants permission to modify the AQUA configuration of a cluster	Write	cluster*		
ModifyAuthenticationProfile	Grants permission to modify an existing Amazon Redshift authentication profile	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyCluster	Grants permission to modify the settings of a cluster	Write	cluster*		acm:DescribeCertificate kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					secretsmanager:GetRandomPassword secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
ModifyClusterDbRevision	Grants permission to modify the database revision of a cluster	Write	cluster*		
ModifyClusterIamRoles	Grants permission to modify the list of Amazon Identity and Access Management (IAM) roles that can be used by a cluster to access other Amazon services	Permissions management	cluster*		
ModifyClusterMaintenance	Grants permission to modify the maintenance settings of a cluster	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyClusterParameterGroup	Grants permission to modify the parameters of a parameter group	Write	parameergroup*		
ModifyClusterSnapshot	Grants permission to modify the settings of a snapshot	Write	snapshot*		
ModifyClusterSnapshotSchedule	Grants permission to modify a snapshot schedule for a cluster	Write	cluster*		
ModifyClusterSubnetGroup	Grants permission to modify a cluster subnet group to include the specified list of VPC subnets	Write	subnetgroup*		
ModifyCustomDomainAssociation	Grants permission to modify a custom domain name for a cluster	Write	cluster*		acm:DescribeCertificate
ModifyEndpointAccess	Grants permission to modify a redshift-managed vpc endpoint	Write			
ModifyEventSubscription	Grants permission to modify an existing Amazon Redshift event notification subscription	Write	eventsubscription*		
ModifyIntegration	Grants permission to modify an Amazon Redshift zero-ETL integration	Write	integration*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
ModifyQev2IdcApplication [permission only]	Grants permission to modify a qev2 idc application	Write	qev2idcapplication*		sso:UpdateApplication

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifyRedshiftIdcApplication	Grants permission to modify a redshift idc application	Write	redshiftidcapplication*		sso:DeleteApplicationAccessScope sso:DeleteApplicationGrant sso:GetApplicationGrant sso:ListApplicationAccessScopes sso:PutApplicationAccessScope sso:PutApplicationGrant sso:UpdateApplication

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifySavedQuery [permission only]	Grants permission to modify an existing saved query through the Amazon Redshift console	Write			
ModifyScheduledAction	Grants permission to modify an existing Amazon Redshift scheduled action	Write			
ModifySnapshotCopyRetentionPeriod	Grants permission to modify the number of days to retain snapshots in the destination Amazon Web Services Region after they are copied from the source Amazon Web Services Region	Write	cluster*		
ModifySnapshotSchedule	Grants permission to modify a snapshot schedule	Write	snapshotschedule*		
ModifyUsageLimit	Grants permission to modify a usage limit	Write	usagelimit*		
PauseCluster	Grants permission to pause a cluster	Write	cluster*		
PurchaseReservedNodeOffering	Grants permission to purchase a reserved node	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutResourcePolicy	Grants permission to update the resource policy for a specified resource	Permissions management	namespace*		
RebootCluster	Grants permission to reboot a cluster	Write	cluster*		
RegisterNamespace	Grants permission to register the specified namespace to a consumer	Write			
RejectDataShare	Grants permission to decline a datashare shared from another account	Permissions management	datashare*		
ResetClusterParameterGroup	Grants permission to set one or more parameters of a parameter group to their default values and set the source values of the parameters to "engine-default"	Write	parameter group*		
ResizeCluster	Grants permission to change the size of a cluster	Write	cluster*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RestoreFromClusterSnapshot	Grants permission to create a cluster from a snapshot	Write	cluster*		kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:GetRandomPassword

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
			snapshot*		
				aws:TagKeys	
RestoreTableFromClusterSnapshot	Grants permission to create a table from a table in an Amazon Redshift cluster snapshot	Write	cluster*		
			snapshot*		
ResumeCluster	Grants permission to resume a cluster	Write	cluster*		
RevokeClusterSecurityGroupIngress	Grants permission to revoke an ingress rule in an Amazon Redshift security group for a previously authorized IP range or Amazon EC2 security group	Write	securitygroup*		
			securitygroupingress-ec2securitygroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RevokeEndpointAccess	Grants permission to revoke access for endpoint related activities for redshift-managed vpc endpoint	Permissions management			
RevokeSnapshotAccess	Grants permission to revoke access from the specified Amazon Web Services account to restore a snapshot	Permissions management	snapshot*		
RotateEncryptionKey	Grants permission to rotate an encryption key for a cluster	Write	cluster*		
UpdatePartnerStatus	Grants permission to update the status of a partner integration	Write			
ViewQueriesFromConsole [permission only]	Grants permission to view query results through the Amazon Redshift console	List			
ViewQueriesInConsole [permission only]	Grants permission to terminate running queries and loads through the Amazon Redshift console	List			

Resource types defined by Amazon Redshift

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:${Partition}:redshift:${Region}:${Account}:cluster:${ClusterName}`	aws:ResourceTag/${TagKey}
datashare	`arn:${Partition}:redshift:${Region}:${Account}:datashare:${ProducerClusterNamespace}/${DataShareName}`	aws:ResourceTag/${TagKey}
dbgroup	`arn:${Partition}:redshift:${Region}:${Account}:dbgroup:${ClusterName}/${DbGroup}`	
dbname	`arn:${Partition}:redshift:${Region}:${Account}:dbname:${ClusterName}/${DbName}`	
dbuser	`arn:${Partition}:redshift:${Region}:${Account}:dbuser:${ClusterName}/${DbUser}`	
eventsubscription	`arn:${Partition}:redshift:${Region}:${Account}:eventsubscription:${EventSubscriptionName}`	aws:ResourceTag/${TagKey}
hsmclientcertificate	`arn:${Partition}:redshift:${Region}:${Account}:hsmclientcertificate:${HSMClientCertificateId}`	aws:ResourceTag/${TagKey}
hsmconfiguration	`arn:${Partition}:redshift:${Region}:${Account}:hsmconfiguration:${HSMConfigurationId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
integration	arn:${Partition}:redshift:${Region}:${Account}:integration:${IntegrationIdentifier}	aws:ResourceTag/${TagKey}
namespace	arn:${Partition}:redshift:${Region}:${Account}:namespace:${ClusterNamespace}	aws:ResourceTag/${TagKey}
parameter group	arn:${Partition}:redshift:${Region}:${Account}:parametergroup:${ParameterGroupName}	aws:ResourceTag/${TagKey}
securitygroup	arn:${Partition}:redshift:${Region}:${Account}:securitygroup:${SecurityGroupName}/ec2securitygroup/${Owner}/${Ec2SecurityGroupId}	aws:ResourceTag/${TagKey}
securitygroupingress-cidr	arn:${Partition}:redshift:${Region}:${Account}:securitygroupingress:${SecurityGroupName}/cidrip/${IpRange}	aws:ResourceTag/${TagKey}
securitygroupingress-ec2securitygroup	arn:${Partition}:redshift:${Region}:${Account}:securitygroupingress:${SecurityGroupName}/ec2securitygroup/${Owner}/${Ece2SecuritygroupId}	aws:ResourceTag/${TagKey}
snapshot	arn:${Partition}:redshift:${Region}:${Account}:snapshot:${ClusterName}/${SnapshotName}	aws:ResourceTag/${TagKey}
snapshotcopygrant	arn:${Partition}:redshift:${Region}:${Account}:snapshotcopygrant:${SnapshotCopyGrantName}	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
snapshotschedule	`arn:${Partition}:redshift:${Region}:${Account}:snapshotschedule:${ScheduleIdentifier}`	aws:ResourceTag/${TagKey}
subnetgroup	`arn:${Partition}:redshift:${Region}:${Account}:subnetgroup:${SubnetGroupName}`	aws:ResourceTag/${TagKey}
usagelimit	`arn:${Partition}:redshift:${Region}:${Account}:usagelimit:${UsageLimitId}`	aws:ResourceTag/${TagKey}
redshiftidcapplication	`arn:${Partition}:redshift:${Region}:${Account}:redshiftidcapplication:${RedshiftIdcApplicationId}`	
qev2idcapplication	`arn:${Partition}:redshift:${Region}:${Account}:qev2idcapplication:${Qev2IdcApplicationId}`	

Condition keys for Amazon Redshift

Amazon Redshift 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 Amazon global condition context keys.

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

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by actions based on tag-value associated with the resource	String
aws:TagKeys	Filters access by actions based on the presence of mandatory tags in the request	ArrayOfString
redshift:AllowWrites	Filters access by the allowWrites input parameter	Bool
redshift:ConsumerArn	Filters access by the datashare consumer arn	ARN
redshift:ConsumerIdentifier	Filters access by the datashare consumer	String
redshift:DbName	Filters access by the database name	String
redshift:DbUser	Filters access by the database user name	String
redshift:DurationSeconds	Filters access by the number of seconds until a temporary credential set expires	String
redshift:InboundIntegrationArn	Filters access by the ARN of an inbound zero-ETL Integration resource	ARN
redshift:IntegrationSourceArn	Filters access by the ARN of a zero-ETL Integration source	ARN
redshift:IntegrationTargetArn	Filters access by the ARN of a zero-ETL Integration target	ARN

Actions, resources, and condition keys for Amazon Redshift Data API

Amazon Redshift Data API (service prefix: `redshift-data`) 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 Redshift Data API
- Resource types defined by Amazon Redshift Data API
- Condition keys for Amazon Redshift Data API

Actions defined by Amazon Redshift Data 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 Amazon. 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.

> **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
BatchExecuteStatement	Grants permission to execute multiple queries under a single connection	Write	cluster		
			workgroup		
				redshift-data:session-owner-iam-user id redshift-data:glue-catalog-arn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelStatement	Grants permission to cancel a running query	Write		redshift-data:statement-owner-iam-userid	
DescribeStatement	Grants permission to retrieve detailed information about a statement execution	Read		redshift-data:statement-owner-iam-userid	
DescribeTable	Grants permission to retrieve metadata about a particular table	Read	cluster*		
			workgroup*		
ExecuteStatement	Grants permission to execute a query	Write	cluster		
			workgroup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				redshift-data:session-owner-iam-userid redshift-data:glue-catalog-arn	
GetStagingBucketLocation	Grants permission to get staging bucket location for a given managed workgroup	Read	managed-workgroup*		
GetStatementResult	Grants permission to fetch the result of a query	Read		redshift-data:statement-owner-iam-userid	
ListDatabases	Grants permission to list databases for a given cluster	Read	cluster*		
			workgroup*		
ListSchemas	Grants permission to list schemas for a given cluster	Read	cluster*		
			workgroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListStatements	Grants permission to list queries for a given principal	List		redshift-data:statement-owner-iam-userid	
ListTables	Grants permission to list tables for a given cluster	List	cluster*		
			workgroup*		

Resource types defined by Amazon Redshift Data API

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:${Partition}:redshift:${Region}:${Account}:cluster:${ClusterName}`	aws:ResourceTag/${TagKey}
workgroup	`arn:${Partition}:redshift-serverless:${Region}:${Account}:workgroup/${WorkgroupId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
managed-workgroup	`arn:${Partition}:redshift-serverless:${Region}:${Account}:managed-workgroup/${ManagedWorkgroupId}`	

Condition keys for Amazon Redshift Data API

Amazon Redshift Data API 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 Amazon global condition context keys.

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by tag-value associated with the resource	String
redshift-data:glue-catalog-arn	Filters access by glue catalog arn	ARN
redshift-data:session-owner-iam-userid	Filters access by session owner iam userid	String
redshift-data:statement-owner-iam-userid	Filters access by statement owner iam userid	String

Actions, resources, and condition keys for Amazon Redshift Serverless

Amazon Redshift Serverless (service prefix: `redshift-serverless`) 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 Redshift Serverless
- Resource types defined by Amazon Redshift Serverless
- Condition keys for Amazon Redshift Serverless

Actions defined by Amazon Redshift Serverless

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 Amazon. 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.

> **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
ConvertRecoveryPointToSnapshot	Grants permission to convert a recovery point to a snapshot	Write	recoveryPoint*		
			snapshot*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateCustomDomainAssociation	Grants permission to create a custom domain association in Amazon Redshift Serverless	Write	workgroup*		acm:DescribeCertificate

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateEndpointAccess	Grants permission to create an Amazon Redshift Serverless managed VPC endpoint	Write	endpointAccess*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateNamespace	Grants permission to create an Amazon Redshift Serverless namespace	Write	namespace*		kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:GetRandomPassword

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateReservation	Grants permission to purchase a capacity reservation according to a specific reservation offering, for a specified number of RPUs	Write			
CreateScheduledAction	Grants permission to create a scheduled action for a specified Amazon Redshift Serverless namespace	Write	namespace*		
CreateSnapshot	Grants permission to create a snapshot of all databases in a namespace	Write	snapshot*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSnapshotCopyConfiguration	Grants permission to create a snapshot copy configuration for a specified Amazon Redshift Serverless namespace	Write	namespace*		
CreateUsageLimit	Grants permission to create a usage limit for a specified Amazon Redshift Serverless usage type	Write			
CreateWorkgroup	Grants permission to create a workgroup in Amazon Redshift Serverless	Write	workgroup*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteCustomDomainAssociation	Grants permission to delete a custom domain association	Write	workgroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteEndpointAccess	Grants permission to delete an Amazon Redshift Serverless managed VPC endpoint	Write	endpointAccess*		
DeleteNamespace	Grants permission to delete a namespace from Amazon Redshift Serverless	Write	namespace*		kms:DescribeKey kms:RetireGrant secretsmanager:DeleteSecret secretsmanager:DescribeSecret
DeleteResourcePolicy	Grants permission to delete the specified resource policy	Write			
DeleteScheduledAction	Grants permission to delete a scheduled action from Amazon Redshift Serverless	Write			
DeleteSnapshot	Grants permission to delete a snapshot from Amazon Redshift Serverless	Write	snapshot*		
DeleteSnapshotCopyConfiguration	Grants permission to delete a snapshot copy configuration for a Amazon Redshift Serverless namespace	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteUsageLimit	Grants permission to delete a usage limit from Amazon Redshift Serverless	Write			
DeleteWorkgroup	Grants permission to delete a workgroup	Write	workgroup*		
DescribeOneTimeCredit [permission only]	Grants permission to see on the Amazon Redshift Serverless console the remaining number of free trial credits and their expiration date	Read			
GetCredentials	Grants permission to get a database user name and temporary password with temporary authorization to log on to Amazon Redshift Serverless	Write	workgroup*		
GetCustomDomainAssociation	Grants permission to get information about a specific custom domain association	Read	workgroup*		
GetEndpointAccess	Grants permission to create an Amazon Redshift Serverless managed VPC endpoint	Read	endpointAccess*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetManagedWorkgroup	Grants permission to create a Amazon Redshift Managed Serverless workgroup with the specified configuration settings	Read	managed-workgroup*		
GetNamespace	Grants permission to get information about a namespace in Amazon Redshift Serverless	Read	namespace*		
GetRecoveryPoint	Grants permission to get information about a recovery point	Read	recoveryPoint*		
GetReservation	Grants permission to get a particular reservation object	Read			
GetReservationOffering	Grants permission to get a particular reservation offering	Read			
GetResourcePolicy	Grants permission to get a resource policy	Read			
GetScheduledAction	Grants permission to get information about a specific scheduled action	Read			
GetSnapshot	Grants permission to get information about a specific snapshot	Read	snapshot*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTableRestoreStatus	Grants permission to get table restore status about a specific snapshot	Read			
GetTrack	Grants permission to get information about a track in Amazon Redshift Serverless	Read			
GetUsageLimit	Grants permission to get information about a usage limit in Amazon Redshift Serverless	Read			
GetWorkgroup	Grants permission to get information about a specific workgroup	Read	workgroup*		
ListCustomDomainAssociations	Grants permission to list custom domain associations in Amazon Redshift Serverless	List			
ListEndpointAccess	Grants permission to list EndpointAccess objects and relevant information	List	endpointAccess*		
ListManagedWorkgroups	Grants permission to list managed workgroups in Amazon Redshift Serverless	List			
ListNamespaces	Grants permission to list namespaces in Amazon Redshift Serverless	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListRecoveryPoints	Grants permission to list an array of recovery points	List	namespace		
ListReservationOfferings	Grants permission to list all available capacity reservation offerings	List			
ListReservations	Grants permission to list all reservations	List			
ListScheduledActions	Grants permission to list scheduled actions	List			
ListSnapshotCopyConfigurations	Grants permission to list SnapshotCopyConfiguration objects and relevant information	List	namespace		
ListSnapshots	Grants permission to list snapshots	List	snapshot*		
ListTableRestoreStatus	Grants permission to list table restore status	List			
ListTagsForResource	Grants permission to list the tags assigned to a resource	List	namespace		
			workgroup		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTracks	Grants permission to list tracks available in Amazon Redshift Serverless	List			
ListUsageLimits	Grants permission to list all usage limits within Amazon Redshift Serverless	List			
ListWorkgroups	Grants permission to list workgroups in Amazon Redshift Serverless	List			
PutResourcePolicy	Grants permission to create or update a resource policy	Write			
RestoreFromRecoveryPoint	Grants permission to restore the data from a recovery point	Write	recoveryPoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RestoreFromSnapshot	Grants permission to restore a namespace from a snapshot	Write	snapshot*		kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:GetRandomPassword

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
RestoreTableFromRecoveryPoint	Grants permission to restore a table from a recovery point	Write	namespace*		
			recoveryPoint*		
RestoreTableFromSnapshot	Grants permission to restore a table from a snapshot	Write	namespace*		
			snapshot*		
TagResource	Grants permission to assign one or more tags to a resource	Tagging	namespace		
			recoveryPoint		
			snapshot		
			workgroup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey}	
UntagResource	Grants permission to remove a tag or set of tags from a resource	Tagging	namespace		
			recoveryPoint		
			snapshot		
			workgroup		
				aws:TagKeys	
UpdateCustomDomainAssociation	Grants permission to update a certificate associated with a custom domain	Write	workgroup*		acm:DescribeCertificate
UpdateEndpointAccess	Grants permission to update an Amazon Redshift Serverless managed VPC endpoint	Write	endpointAccess*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateNamespace	Grants permission to update a namespace with the specified configuration settings	Write	namespace*		kms:CreateGrant kms:Decrypt kms:DescribeKey kms:GenerateDataKey kms:RetireGrant secretsmanager:CreateSecret secretsmanager:DeleteSecret secretsmanager:DescribeSecret secretsmanager:GetRandomPassword

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					secretsmanager:RotateSecret secretsmanager:TagResource secretsmanager:UpdateSecret
UpdateScheduledAction	Grants permission to update a scheduled action	Write			
UpdateSnapshot	Grants permission to update a snapshot	Write	snapshot*		
UpdateSnapshotCopyConfiguration	Grants permission to update a snapshot copy configuration for a Amazon Redshift Serverless namespace	Write			
UpdateUsageLimit	Grants permission to update a usage limit in Amazon Redshift Serverless	Write			
UpdateWorkgroup	Grants permission to update an Amazon Redshift Serverless workgroup with the specified configuration settings	Write	workgroup*		

Resource types defined by Amazon Redshift Serverless

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
namespace	`arn:${Partition}:redshift-serverless:${Region}:${Account}:namespace/${NamespaceId}`	aws:ResourceTag/${TagKey}
snapshot	`arn:${Partition}:redshift-serverless:${Region}:${Account}:snapshot/${SnapshotId}`	aws:ResourceTag/${TagKey}
workgroup	`arn:${Partition}:redshift-serverless:${Region}:${Account}:workgroup/${WorkgroupId}`	aws:ResourceTag/${TagKey}
managed-workgroup	`arn:${Partition}:redshift-serverless:${Region}:${Account}:managed-workgroup/${ManagedWorkgroupName}`	
recoveryPoint	`arn:${Partition}:redshift-serverless:${Region}:${Account}:recoverypoint/${RecoveryPointId}`	aws:ResourceTag/${TagKey}
endpointAccess	`arn:${Partition}:redshift-serverless:${Region}:${Account}:managedvpcendpoint/${EndpointAccessId}`	

Condition keys for Amazon Redshift Serverless

Amazon Redshift Serverless 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 Amazon 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
redshift-serverless:endpointAccessId	Filters access by the endpoint access identifier	String
redshift-serverless:managedWorkgroupName	Filters access by the managed workgroup identifier	String
redshift-serverless:namespaceId	Filters access by the namespace identifier	String
redshift-serverles	Filters access by the recovery point identifier	String

Condition keys	Description	Type
s:recoveryPointId		
redshift-serverless:snapshotId	Filters access by the snapshot identifier	String
redshift-serverless:tableRestoreRequestId	Filters access by the table restore request identifier	String
redshift-serverless:workgroupId	Filters access by the workgroup identifier	String

Actions, resources, and condition keys for Amazon Resource Access Manager (RAM)

Amazon 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 Amazon Resource Access Manager (RAM)
- Resource types defined by Amazon Resource Access Manager (RAM)
- Condition keys for Amazon Resource Access Manager (RAM)

Actions defined by Amazon 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 Amazon. 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.

> **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/${TagKey} ram:ResourceTag/${TagKey} ram:ResourceShareName ram:AllowsExternalPrincipals	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ram:Principal ram:RequestedResourceType ram:ResourceArn	
AssociateResourceSharePermission	Grants permission to associate a Permission with a Resource Share	Write	customer-managed-permission*		
			permission*		
			resource-share*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
				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 Amazon 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 Amazon RAM permission	List			
ListPermissions	Grants permission to list the Amazon 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 Amazon 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 Amazon 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 Amazon Resource Access Manager (RAM)

Amazon 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 Amazon 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 Amazon accounts that are outside of its Amazon 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 Amazon accounts that are outside of its Amazon 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 Amazon. 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.

> **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 Amazon Web Services Region for the calling account	Read			
GetTagKeys	Grants permission to returns tag keys currently in use in the specified Amazon Web Services Region for the calling account	Read			
GetTagValues	Grants permission to return tag values for the specified key that are used in the specified Amazon Web Services Region for the calling account	Read			
StartReportCreation	Grants permission to start generating a report listing all	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	tagged resources in accounts across your organization, and whether each resource is compliant with the effective tag policy				
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 Amazon global condition context keys.

Actions, resources, and condition keys for Amazon Resource Groups

Amazon 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 Amazon Resource Groups
- Resource types defined by Amazon Resource Groups
- Condition keys for Amazon Resource Groups

Actions defined by Amazon 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 Amazon. 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.

> **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*		
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	Grants permission to delete a resource-based policy for the specified group	Write	group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
[permission only]					
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*		
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*		

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
PutGroupPolicy [permission only]	Grants permission to add a resource-based policy for the specified group	Write	group*		
SearchResources	Grants permission to search for Amazon resources matching the given query	List			cloudformation:DescribeStacks cloudformation:ListStackResources tag:GetResources

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 Amazon 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 Amazon Resource Groups

Amazon 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 Amazon 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 Amazon. 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.

> **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*		
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:ChangeReso	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				urceRecordSetsActions	
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			
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*		

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateVPCAssociationAuthorization	Grants permission to authorize the Amazon Web Services account that created a specified VPC to submit an AssociateVPCWithHostedZone 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*		
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*		

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetHealthCheckCount	Grants permission to get the number of health checks that are associated with the current Amazon Web Services 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*		
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 Amazon Web Services account	List			
GetHostedZoneLimit	Grants permission to get the specified limit for a specified hosted zone	Read	hostedzone*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetQueryLoggingConfig	Grants permission to get information about a specified configuration for DNS query logging	Read	querylogging config*		
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*		
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 Amazon Web Services account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 Amazon Web Services 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			
ListHealthChecks	Grants permission to get a list of the health checks that are associated with the current Amazon Web Services account	Read			
ListHostedZones	Grants permission to get a list of the public and private hosted zones that are associated with the current Amazon Web Services account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 Amazon Web Services account or the configuration that is associated with a specified hosted zone	List	hostedzone		
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 Amazon Web Services account.	Read			
ListTagsForResource	Grants permission to list tags for one health check or hosted zone	Read	healthcheck		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			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 Amazon Web Services account. Policies are listed in the order in which they were created	List			
ListTrafficPolicyInstances	Grants permission to get information about the traffic policy instances that you created by using the current Amazon Web Services account	Read			
ListTrafficPolicyInstancesByHostedZone	Grants permission to get information about the traffic policy instances that you created in a specified hosted zone	List	hostedzone*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		
UpdateTrafficPolicyComment	Grants permission to update the comment for a specified traffic policy version	Write	trafficpolicy*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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}`	

Resource types	ARN	Condition keys
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 Amazon 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

Condition keys	Description	Type
route53:ChangeResourceRecordSetsRecordTypes	Filters access by the DNS record types in a ChangeResourceRecordSets request	ArrayOfString
route53:VPCs	Filters access by VPCs in request	ArrayOfString

Actions, resources, and condition keys for Amazon Route 53 Profiles

Amazon Route 53 Profiles (service prefix: `route53profiles`) 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 Profiles
- Resource types defined by Amazon Route 53 Profiles
- Condition keys for Amazon Route 53 Profiles

Actions defined by Amazon Route 53 Profiles

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 Amazon. 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.

> **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 Profile	Grants permission to associates a Profile to the customer VPC	Write		aws:RequestTag/${TagKey}	ec2:DescribeVpcs

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
AssociateResourceToProfile	Grants permission to associates a resource, such as DNS Firewall rule group, private hosted zone, resolver rule, etc. to a specified Profile	Write			
CreateProfile	Grants permission to create a new Profile resource	Write		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteProfile	Grants permission to delete a Profile specified by the ProfileId	Write			
DisassociateProfile	Grants permission to delete an association between a customer VPC and the specified Profile	Write			
DisassociateResourceFromProfile	Grants permission to delete the asoociation between the resource. such as DNS Firewall rule group, private hosted zone, resolver rule, etc. and the specified Profile	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetProfile	Grants permission to get a Profile	Read			
GetProfileAssociation	Grants permission to get a Profile to a VPC association specified by the Profile association ID	Read			
GetProfilePolicy [permission only]	Grants permission to read the RAM access control policy for a Profile	Read	profile*		
GetProfileResourceAssociation	Grants permission to get a Profile resource association based on the ProfileResourceAssociationId	Read			
ListProfileAssociations	Grants permission to list all VPCs the specified Profile is associated to	List			
ListProfileResourceAssociations	Grants permission to list all the associations between the resources, such as DNS Firewall rule groups, private hosted zones, resolver rules, etc. for the given Profile ID	List			
ListProfiles	Grants permission to list all the Profiles created by, and shared to the customer	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to list all tags associated with the resource	List			
PutProfilePolicy [permission only]	Grants permission to define the RAM access control policy for a Profile	Write	profile*		
TagResource	Grants permission to add a tag to the given resource	Tagging	profile		
			profile-association		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to delete a tag from the given resource	Tagging	profile		
			profile-association		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateProfileResourceAssociation	Grants permission to update the Profile resource association name or the resource properties or both, if both name and resource properties are null, the api returns the existing Profile resource association	Write			

Resource types defined by Amazon Route 53 Profiles

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
profile	`arn:${Partition}:route53profiles:${Region}:${Account}:profile/${ResourceId}`	aws:ResourceTag/${TagKey}
profile-association	`arn:${Partition}:route53profiles:${Region}:${Account}:profile-association/${ResourceId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Route 53 Profiles

Amazon Route 53 Profiles 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 Amazon 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 the presence of 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 Resolver

Amazon Route 53 Resolver (service prefix: `route53resolver`) 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 Resolver
- Resource types defined by Amazon Route 53 Resolver
- Condition keys for Amazon Route 53 Resolver

Actions defined by Amazon Route 53 Resolver

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 Amazon. 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.

> **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
AssociateFirewallRuleGroup	Grants permission to associate an Amazon VPC with a specified firewall rule group	Write	firewall-rule-group-association*		ec2:DescribeVpcs
				aws:RequestTag/${TagKey} aws:TagKeys	
AssociateResolverEndpointIpAddress	Grants permission to associate a specified IP address with a Resolver endpoint. This is an IP address that DNS queries pass through on the way to your network (outbound) or your VPCs (inbound)	Write	resolver-endpoint*		ec2:CreateNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSubnets
AssociateResolverQueryLogConfig	Grants permission to associate an Amazon VPC with a specified query logging configuration	Write	resolver-query-log-config*		ec2:DescribeVpcs

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AssociateResolverRule	Grants permission to associate a specified Resolver rule with a specified VPC	Write	resolver-rule*		ec2:DescribeVpcs
CreateFirewallDomainList	Grants permission to create a Firewall domain list	Write	firewall-domain-list*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateFirewallRule	Grants permission to create a Firewall rule within a Firewall rule group	Write	firewall-domain-list*		
			firewall-rule-group*		
CreateFirewallRuleGroup	Grants permission to create a Firewall rule group	Write	firewall-rule-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateOutpostResolver	Grants permission to create a Route 53 Resolver on Outposts	Write	outpost-resolver*		outposts:GetOutpost
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateResolverEndpoint	Grants permission to create a Resolver endpoint. There are two types of Resolver endpoints, inbound and outbound	Write	resolver-endpoint*		ec2:CreateNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:DescribeVpcs
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateResolverQueryLogConfig	Grants permission to create a Resolver query logging configuration, which defines where you want Resolver to save DNS query logs that originate in your VPCs	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateResolverRule	Grants permission to define how to route queries originating from your VPC out of the VPC	Write	resolver-rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteFirewallDomainList	Grants permission to delete a Firewall domain list	Write	firewall-domain-list*		
DeleteFirewallRule	Grants permission to delete a Firewall rule within a Firewall rule group	Write	firewall-domain-list*		
			firewall-rule-group*		
DeleteFirewallRuleGroup	Grants permission to delete a Firewall rule group	Write	firewall-rule-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteOutpostResolver	Grants permission to delete a Route 53 Resolver on Outposts	Write	outpost-resolver*		
DeleteResolverEndpoint	Grants permission to delete a Resolver endpoint. The effect of deleting a Resolver endpoint depends on whether it's an inbound or an outbound endpoint	Write	resolver-endpoint*		ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces
DeleteResolverQueryLogConfig	Grants permission to delete a Resolver query logging configuration	Write	resolver-query-log-config*		
DeleteResolverRule	Grants permission to delete a Resolver rule	Write	resolver-rule*		
DisassociateFirewallRuleGroup	Grants permission to remove the association between a specified Firewall rule group and a specified VPC	Write	firewall-rule-group-association*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DisassociateResolverEndpointIpAddress	Grants permission to remove a specified IP address from a Resolver endpoint. This is an IP address that DNS queries pass through on the way to your network (outbound) or your VPCs (inbound)	Write	resolver-endpoint*		ec2:DeleteNetworkInterface ec2:DescribeNetworkInterfaces
DisassociateResolverQueryLogConfig	Grants permission to remove the association between a specified Resolver query logging configuration and a specified VPC	Write	resolver-query-log-config*		
DisassociateResolverRule	Grants permission to remove the association between a specified Resolver rule and a specified VPC	Write	resolver-rule*		
GetFirewallConfig	Grants permission to get information about a specified Firewall config	Read	firewall-config*		ec2:DescribeVpcs
GetFirewallDomainList	Grants permission to get information about a specified Firewall domain list	Read	firewall-domain-list*		
GetFirewallRuleGroup	Grants permission to get information about a specified Firewall rule group	Read	firewall-rule-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetFirewallRuleGroupAssociation	Grants permission to get information about an association between a specified Firewall rule group and a VPC	Read	firewall-rule-group-association*		
GetFirewallRuleGroupPolicy	Grants permission to get information about a specified Firewall rule group policy, which specifies the Firewall rule group operations and resources that you want to allow another Amazon Web Services account to use	Read	firewall-rule-group*		
GetOutpostResolver	Grants permission to get information about a specified Route 53 Resolver on Outposts	Read	outpost-resolver*		
GetResolverConfig	Grants permission to get the Resolver Config status within the specified resource	Read	resolver-config*		ec2:DescribeVpcs
GetResolverDnssecConfig	Grants permission to get the DNSSEC validation support status for DNS queries within the specified resource	Read	resolver-dnssec-config*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetResolverEndpoint	Grants permission to get information about a specified Resolver endpoint, such as whether it's an inbound or an outbound endpoint, and the IP addresses in your VPC that DNS queries are forwarded to on the way into or out of your VPC	Read	resolver-endpoint*		
GetResolverQueryLogConfig	Grants permission to get information about a specified Resolver query logging configuration, such as the number of VPCs that the configuration is logging queries for and the location that logs are sent to	Read	resolver-query-log-config*		ec2:DescribeVpcs
GetResolverQueryLogConfigAssociation	Grants permission to get information about a specified association between a Resolver query logging configuration and an Amazon VPC. When you associate a VPC with a query logging configuration, Resolver logs DNS queries that originate in that VPC	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetResolverQueryLogConfigPolicy	Grants permission to get information about a specified Resolver query logging policy, which specifies the Resolver query logging operations and resources that you want to allow another Amazon Web Services account to use	Read	resolver-query-log-config*		
GetResolverRule	Grants permission to get information about a specified Resolver rule, such as the domain name that the rule forwards DNS queries for and the IP address that queries are forwarded to	Read	autodefined-rule		
			resolver-rule		
GetResolverRuleAssociation	Grants permission to get information about an association between a specified Resolver rule and a VPC	Read	autodefined-rule		
			resolver-rule		
GetResolverRulePolicy	Grants permission to get information about a Resolver rule policy, which specifies the Resolver operations and resources that you want to allow another Amazon Web Services account to use	Read	resolver-rule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportFirewallDomains	Grants permission to add, remove or replace Firewall domains in a Firewall domain list	Write	firewall-domain-list*		
ListFirewallConfigs	Grants permission to list all the Firewall config that current Amazon Web Services account is able to check	List			ec2:DescribeVpcs
ListFirewallDomainLists	Grants permission to list all the Firewall domain list that current Amazon Web Services account is able to use	List			
ListFirewallDomains	Grants permission to list all the Firewall domain under a specified Firewall domain list	List	firewall-domain-list*		
ListFirewallRuleGroupAssociations	Grants permission to list information about associations between Amazon VPCs and Firewall rule group	List			
ListFirewallRuleGroups	Grants permission to list all the Firewall rule group that current Amazon Web Services account is able to use	List			
ListFirewallRules	Grants permission to list all the Firewall rule under a specified Firewall rule group	List	firewall-rule-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListOutpostResolvers	Grants permission to list all instances of Route 53 Resolver on Outposts that were created using the current Amazon Web Services account	List			
ListResolverConfigs	Grants permission to list Resolver Config statuses	List	resolver-config*		ec2:DescribeVpcs
ListResolverDnssecConfigs	Grants permission to list the DNSSEC validation support status for DNS queries	List	resolver-dnssec-config*		
ListResolverEndpointIpAddresses	Grants permission to list the IP addresses that DNS queries pass through on the way to your network (outbound) or your VPCs (inbound) for a specified Resolver endpoint	List	resolver-endpoint*		
ListResolverEndpoints	Grants permission to list all the Resolver endpoints that were created using the current Amazon Web Services account	List			
ListResolverQueryLogConfigAssociations	Grants permission to list information about associations between Amazon VPCs and query logging configurations	List			ec2:DescribeVpcs

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListResolverQueryLogConfigs	Grants permission to list information about the specified query logging configurations, which define where you want Resolver to save DNS query logs and specify the VPCs that you want to log queries for	List			ec2:DescribeVpcs
ListResolverRuleAssociations	Grants permission to list the associations that were created between Resolver rules and VPCs using the current Amazon Web Services account	List			ec2:DescribeVpcs
ListResolverRules	Grants permission to list the Resolver rules that were created using the current Amazon Web Services account	List			
ListTagsForResource	Grants permission to list the tags that you associated with the specified resource	Read	firewall-domain-list		
			firewall-rule-group		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			firewall-rule-group-association		
			outpost-resolver		
			resolver-endpoint		
			resolver-query-log-config		
			resolver-rule		
PutFirewallRuleGroupPolicy	Grants permission to specify an Amazon Web Services account that you want to share a Firewall rule group with, the Firewall rule group that you want to share, and the operations that you want the account to be able to perform on the configuration	Permissions management	firewall-rule-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutResolverQueryLogConfigPolicy	Grants permission to specify an Amazon Web Services account that you want to share a query logging configuration with, the query logging configuration that you want to share, and the operations that you want the account to be able to perform on the configuration	Permissions management	resolver-query-log-config*		
PutResolverRulePolicy	Grants permission to specify an Amazon Web Services account that you want to share rules with, the Resolver rules that you want to share, and the operations that you want the account to be able to perform on those rules	Permissions management	resolver-rule*		
TagResource	Grants permission to add one or more tags to a specified resource	Tagging	firewall-config		
			firewall-domain-list		
			firewall-rule-group		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			firewall-rule-group-association		
			outpost-resolver		
			resolver-dnssec-config		
			resolver-endpoint		
			resolver-query-log-config		
			resolver-rule		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove one or more tags from a specified resource	Tagging	firewall-config		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			firewall-domain-list		
			firewall-rule-group		
			firewall-rule-group-association		
			outpost-resolver		
			resolver-dnssec-config		
			resolver-endpoint		
			resolver-query-log-config		
			resolver-rule		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateFirewallConfig	Grants permission to update selected settings for an Firewall config	Write	firewall-config*		ec2:DescribeVpcs
UpdateFirewallDomains	Grants permission to add, remove or replace Firewall domains in a Firewall domain list	Write	firewall-domain-list*		
UpdateFirewallRule	Grants permission to update selected settings for an Firewall rule in a Firewall rule group	Write	firewall-domain-list*		
			firewall-rule-group*		
UpdateFirewallRuleGroupAssociation	Grants permission to update selected settings for an Firewall rule group association	Write	firewall-rule-group-association*		
UpdateOutpostResolver	Grants permission to update seletected settings for a specified Route 53 Resolver on Outposts	Write	outpost-resolver*		
UpdateResolverConfig	Grants permission to update the Resolver Config status within the specified resource	Write	resolver-config*		ec2:DescribeVpcs

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateResolverDnssecConfig	Grants permission to update the DNSSEC validation support status for DNS queries within the specified resource	Write	resolver-dnssec-config*		
UpdateResolverEndpoint	Grants permission to update selected settings for an inbound or an outbound Resolver endpoint	Write	resolver-endpoint*		ec2:AssignIpv6Addresses ec2:DescribeNetworkInterfaces ec2:DescribeSubnets ec2:ModifyNetworkInterfaceAttribute ec2:UnassignIpv6Addresses
UpdateResolverRule	Grants permission to update settings for a specified Resolver rule	Write	resolver-rule*		

Resource types defined by Amazon Route 53 Resolver

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
resolver-dnssec-config	`arn:${Partition}:route53resolver:${Region}:${Account}:resolver-dnssec-config/${ResourceId}`	aws:ResourceTag/${TagKey}
resolver-query-log-config	`arn:${Partition}:route53resolver:${Region}:${Account}:resolver-query-log-config/${ResourceId}`	aws:ResourceTag/${TagKey}
resolver-rule	`arn:${Partition}:route53resolver:${Region}:${Account}:resolver-rule/${ResourceId}`	aws:ResourceTag/${TagKey}
autodefined-rule	`arn:${Partition}:route53resolver:${Region}:${Account}:autodefined-rule/${ResourceId}`	aws:ResourceTag/${TagKey}
resolver-endpoint	`arn:${Partition}:route53resolver:${Region}:${Account}:resolver-endpoint/${ResourceId}`	aws:ResourceTag/${TagKey}
firewall-rule-group	`arn:${Partition}:route53resolver:${Region}:${Account}:firewall-rule-group/${ResourceId}`	aws:ResourceTag/${TagKey}
firewall-rule-group-association	`arn:${Partition}:route53resolver:${Region}:${Account}:firewall-rule-group-association/${ResourceId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
firewall-domain-list	`arn:${Partition}:route53resolver:${Region}:${Account}:firewall-domain-list/${ResourceId}`	aws:ResourceTag/${TagKey}
firewall-config	`arn:${Partition}:route53resolver:${Region}:${Account}:firewall-config/${ResourceId}`	aws:ResourceTag/${TagKey}
resolver-config	`arn:${Partition}:route53resolver:${Region}:${Account}:resolver-config/${ResourceId}`	
outpost-resolver	`arn:${Partition}:route53resolver:${Region}:${Account}:outpost-resolver/${ResourceId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Route 53 Resolver

Amazon Route 53 Resolver 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 Amazon 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 the presence of tag key-value pairs attached to the resource	String

Condition keys	Description	Type
aws:TagKeys	Filters access by the presence of tag keys in the request	ArrayOfString

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 Amazon. 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.

> **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	object*		
				s3:DataAccessPointArn s3:AccessGrantsInstanceArn	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:AccessPointNetworkOrigin s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
AssociateAccessGrantsIdentityCenter	Grants permission to associate 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}	
BypassGovernanceRetention	Grants permission to allow circumvention of governance-mode object retention settings	Permissions management	object*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:RequestObjectTag/<key> s3:RequestObjectTagKeys s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:TlsVersion s3:x-amz-acl s3:x-amz-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-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				grant-write s3:x-amz-grant-write-acp 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-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				encryption-customer-algorithm s3:x-amz-storage-class s3:x-amz-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:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateBucketMetadataTableConfiguration	Grants permission to create a new S3 Metadata configuration for a specified bucket	Write	bucket*		s3tables:CreateNamespace s3tables:CreateTable s3tables:GetTable 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 managemet	accessgrant*		

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}	
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: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
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
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 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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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	object*		
				s3:AccessGrantsInstanceArn s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin 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	
DeleteObjectTagging	Grants permission to use the tagging subresource to remove the entire tag set from the specified object	Tagging	object*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:ExistingObjectTag/<key> 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	
DeleteObjectVersion	Grants permission to remove a specific version of an object	Write	object*		

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:versionid	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:x-amz-content-sha256	
DeleteObjectVersionTagging	Grants permission to remove the entire tag set for a specific version of the object	Tagging	object*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:versionid	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:x-amz-content-sha256	
DeleteStorageLensConfiguration	Grants permission to delete an existing Amazon S3 Storage Lens configuration	Write	storagelensconfiguration*		
				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: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: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
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
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
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 Amazon Web Services 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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetBucketAcl	Grants permission to use the acl subresource to return the access control list (ACL) of 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
GetBucketCORS	Grants permission to return the CORS configuration information set for an Amazon S3 bucket	Read	bucket*		
				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	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 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	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	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	object*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:TlsVersion s3:x-amz-content-sha256 s3:if-match s3:if-none-match	
GetObjectAcl	Grants permission to return the access control list (ACL) of an object	Read	object*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:TlsVersion s3:x-amz-content-sha256	
GetObjectAttributes	Grants permission to retrieve attributes related to a specific object	Read	accesspoint*		
			object*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:ExistingObjectTag/<key> 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	
GetObjectLegalHold	Grants permission to get an object's current Legal Hold status	Read	object*		

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
GetObjectRetention	Grants permission to retrieve the retention settings for an object	Read	object*		
				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
GetObjectTagging	Grants permission to return the tag set of an object	Read	object*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:ExistingObjectTag/<key> 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	
GetObjectTorrent	Grants permission to return torrent files from an Amazon S3 bucket	Read	object*		
				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	object*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:TlsVersion s3:versionid s3:x-amz-content-sha256	
GetObjectVersionAcl	Grants permission to return the access control list (ACL) of a specific object version	Read	object*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:TlsVersion s3:versionid s3:x-amz-content-sha256	
GetObjectVersionAttributes	Grants permission to retrieve attributes related to a specific version of an object	Read	object*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:versionid	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:x-amz-content-sha256	
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	object*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:versionid	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:x-amz-content-sha256	
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	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:delimiter s3:max-keys s3:prefix s3:ResourceAccount s3:signatureAge	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
ListBucketMultipartUploads	Grants permission to list in-progress multipart uploads	List	bucket*		

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	
ListBucketVersions	Grants permission to list metadata about all the versions of objects in an Amazon S3 bucket	List	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:authType s3:delimiter s3:max-keys s3:prefix s3:ResourceAccount s3:signatureAge	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256	
ListCallerAccessGrants	Grants permission to list caller's 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
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	object*		

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	
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		
			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
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*		

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
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 Amazon Web Services 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	

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	object*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:AccessGrantsInstanceArn s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:RequestObjectTag/<key> s3:RequestObjectTagKeys s3:authType s3:ResourceAccount s3:signatureAge	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:signatureversion s3:TlsVersion s3:x-amz-acl s3:x-amz-content-sha256 s3:x-amz-copy-source s3:x-amz-grant-full-control s3:x-amz-grant-read s3:x-amz-grant-read-acp	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:x-amz-grant-write s3:x-amz-grant-write-acp s3:x-amz-metadata-directive s3:x-amz-server-side-encryption s3:x-amz-server-side-encryption-aws-kms-key-id s3:x-amz-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				server-side-encryption-customer-algorithm s3:x-amz-storage-class s3:x-amz-website-redirect-location 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 s3:object-lock-legal-hold s3:if-match s3:if-none-match s3:ObjectCreationOperation	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutObjectAcl	Grants permission to set the access control list (ACL) permissions for new or existing objects in an S3 bucket	Permissions management	object*		
				s3:AccessGrantsInstanceArn s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:TlsVersion s3:x-amz-acl s3:x-amz-content-sha256 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-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				grant-write-acp s3:x-amz-storage-class	
PutObjectLegalHold	Grants permission to apply a Legal Hold configuration to the specified object	Write	object*		

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:object-lock-legal-hold	
PutObjectRetention	Grants permission to place an Object Retention configuration on an object	Write	object*		

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:object-lock-mode s3:object-lock-retain-until-date s3:object-lock-remaining-retention-days	
PutObjectTagging	Grants permission to set the supplied tag-set to an object that already exists in a bucket	Tagging	object*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:ExistingObjectTag/<key> s3:RequestObjectTag/<key> s3:RequestObjectTagKeys s3:authType s3:ResourceAccount s3:signatureAge	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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	object*		
				s3:AccessGrantsInstanceArn s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:ExistingObjectTag/<key> s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:TlsVersion s3:versionid s3:x-amz-acl s3:x-amz-content-sha256 s3:x-amz-grant-full-control s3:x-amz-grant-read s3:x-amz-grant-read-acp s3:x-amz-grant-write	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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	object*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:DataAccessPointAccount s3:DataAccessPointArn s3:AccessPointNetworkOrigin s3:ExistingObjectTag/<key> s3:RequestObjectTag/<key> s3:RequestObjectTagKeys s3:authType s3:ResourceAccount s3:signatureAge	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3:signatureversion s3:TlsVersion s3:versionid s3:x-amz-content-sha256	
PutReplicationConfiguration	Grants permission to create a new replication configuration or replace an existing one	Write	bucket*		iam:PassRole

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: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	object*		

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
SubmitMultiRegionAccessPointRoutes	Grants permission to submit a route configuration update for a Multi-Region Access Point	Write	multiregionaccesspoint*		
				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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			accessgrantsinstance		
			accessgrantslocation		
			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		
			storagelensgroup		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateAccessGrantsLocation	Grants permission to update Access Grants location	Permissions management	accessgrantslocation*		
				s3:authType s3:ResourceAccount s3:signatureAge s3:signatureversion s3:TlsVersion s3:x-amz-content-sha256 aws:ResourceTag/${TagKey}	
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}	
bucket	arn:${Partition}:s3:::${BucketName}	
object	arn:${Partition}:s3:::${BucketName}/${ObjectName}	
job	arn:${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 Amazon 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:AccessGrantsInstanceArn	Filters access by access grants instance ARN	ARN
s3:AccessPointNetworkOrigin	Filters access by the network origin (Internet or VPC)	String
s3:DataAccessPointAccount	Filters access by the Amazon 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

Condition keys	Description	Type
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
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 Amazon Web Services account ID	String
s3:TlsVersion	Filters access by the TLS version used by the client	Numeric

Condition keys	Description	Type
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 Amazon 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 Amazon 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
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

Condition keys	Description	Type
s3:signatureAge	Filters access by the age in milliseconds of the request signature	Numeric
s3:signatureversion	Filters access by the version of Amazon 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
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

Condition keys	Description	Type
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 Amazon 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 S3 Express

Amazon S3 Express (service prefix: `s3express`) 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 Express
- Resource types defined by Amazon S3 Express
- Condition keys for Amazon S3 Express

Actions defined by Amazon S3 Express

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 Amazon. 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.

> **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
CreateAccessPoint	Grants permission to create a new access point	Write	accesspoint*		
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:LocationName s3express:ResourceAccount	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	
CreateBucket	Grants permission to create a new bucket	Write	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3express:authType s3express:LocationName s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateSession	Grants permission to Create Session token which is used for object APIs such as PutObject, GetObject, ect	Write	bucket*		
				s3express:authType s3express:ResourceAccount s3express:SessionMode s3express:signatureAge s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256 s3express:x-amz-server-side-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				encryption s3express:x-amz-server-side-encryption-aws-kms-key-id s3express:AllAccessRestrictedToLocalZoneGroup	
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
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				content-sha256	
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
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				content-sha256	
DeleteAccessPointScope	Grants permission to delete the scope configuration on a specified access point	Permissions management	accesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				content-sha256	
DeleteBucket	Grants permission to delete the bucket named in the URI	Write	bucket*		
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express: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*		
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAccessPoint	Grants permission to return configuration information about the specified access point	Read		s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				content-sha256	
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
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				content-sha256	
GetAccessPointScope	Grants permission to return the scope configuration associated with the specified access point	Read	accesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				content-sha256	
GetBucketPolicy	Grants permission to return the policy of the specified bucket	Read	bucket*		
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetEncryptionConfiguration	Grants permission to return the default encryption configuration for a directory bucket	Read	bucket*		
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express: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 a directory bucket	Read	bucket*		
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAccessPointsForDirectoryBuckets	Grants permission to list access points	List		s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAllMyDirectoryBuckets	Grants permission to list all directory buckets owned by the authenticated sender of the request	List		s3express:authType s3express:ResourceAccount s3express:signaturversion s3express:TlsVersion s3express:x-amz-content-sha256	
PutAccessPointPolicy	Grants permission to associate an access policy with a specified access point	Permissions managemet	accesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				content-sha256	
PutAccessPointScope	Grants permission to associate an access point with a specified access point scope configuration	Permissions management	accesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3express:DataAccessPointAccount s3express:DataAccessPointArn s3express:AccessPointNetworkOrigin s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				content-sha256	
PutBucketPolicy	Grants permission to add or replace a bucket policy on a bucket	Permissions management	bucket*		
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	
PutEncryptionConfiguration	Grants permission to set the encryption configuration for a directory bucket	Write	bucket*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutLifecycleConfiguration	Grants permission to create a new lifecycle configuration for the directory bucket or replace an existing lifecycle configuration	Write	bucket*		
				s3express:authType s3express:ResourceAccount s3express:signatureversion s3express:TlsVersion s3express:x-amz-content-sha256	

Resource types defined by Amazon S3 Express

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
bucket	`arn:${Partition}:s3express:${Region}:${Account}:bucket/${BucketName}`	
accesspoint	`arn:${Partition}:s3express:${Region}:${Account}:accesspoint/${AccessPointName}`	

Condition keys for Amazon S3 Express

Amazon S3 Express 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 Amazon global condition context keys.

Condition keys	Description	Type
s3express:AccessPointNetworkOrigin	Filters access by the network origin (Internet or VPC)	String
s3express:AllAccessRestrictedToLocalZoneGroup	Filters access by Amazon Local Zone network border group(s) provided in this condition key	String
s3express:DataAccessPointAccount	Filters access by the Amazon Account ID that owns the access point	String

Condition keys	Description	Type
s3express:DataAccessPointArn	Filters access by an access point Amazon Resource Name (ARN)	ARN
s3express:LocationName	Filters access by a specific Availability Zone ID	String
s3express:Permissions	Filters access by the permission requested by Access Point Scope configuration, such as GetObject, PutObject	ArrayOfString
s3express:ResourceAccount	Filters access by the resource owner Amazon Web Services account ID	String
s3express:SessionMode	Filters access by the permission requested by CreateSession API, such as ReadOnly and ReadWrite	String
s3express:TlsVersion	Filters access by the TLS version used by the client	Numeric
s3express:authType	Filters access by authentication method	String
s3express:signatureAge	Filters access by the age in milliseconds of the request signature	Numeric
s3express:signaturversion	Filters access by the Amazon Signature Version used on the request	String
s3express:x-amz-content-sha256	Filters access by unsigned content in your bucket	String
s3express:x-amz-server-side-encryption	Filters access by server-side encryption	String

Condition keys	Description	Type
s3express:x-amz-server-side-encryption-aws-kms-key-id	Filters access by Amazon KMS customer managed key for server-side encryption	ARN

Actions, resources, and condition keys for Amazon S3 Glacier

Amazon S3 Glacier (service prefix: `glacier`) 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 Glacier
- Resource types defined by Amazon S3 Glacier
- Condition keys for Amazon S3 Glacier

Actions defined by Amazon S3 Glacier

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 Amazon. 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.

> **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 identified by the upload ID	Write	vault*		
AbortVaultLock	Grants permission to abort the vault locking process if the vault lock is not in the Locked state	Permissions management	vault*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddTagsToVault	Grants permission to add the specified tags to a vault	Tagging	vault*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CompleteMultipartUpload	Grants permission to complete a multipart upload process	Write	vault*		
CompleteVaultLock	Grants permission to complete the vault locking process	Permissions management	vault*		
CreateVault	Grants permission to create a new vault with the specified name	Write	vault*		
DeleteArchive	Grants permission to delete an archive from a vault	Write	vault*		
				glacier:ArchiveAgeInDays	
DeleteVault	Grants permission to delete a vault	Write	vault*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVaultAccessPolicy	Grants permission to delete the access policy associated with the specified vault	Permissions management	vault*		
DeleteVaultNotifications	Grants permission to delete the notification configuration set for a vault	Write	vault*		
DescribeJob	Grants permission to get information about a job previously initiated	Read	vault*		
DescribeVault	Grants permission to get information about a vault	Read	vault*		
GetDataRetrievalPolicy	Grants permission to get the data retrieval policy	Read			
GetJobOutput	Grants permission to download the output of the job specified	Read	vault*		
GetVaultAccessPolicy	Grants permission to retrieve the access-policy subresource set on the vault	Read	vault*		
GetVaultLock	Grants permission to retrieve attributes from the lock-policy subresource set on the specified vault	Read	vault*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetVaultNotifications	Grants permission to retrieve the notification-configuration subresource set on the vault	Read	vault*		
InitiateJob	Grants permission to initiate a job of the specified type	Write	vault*		
				glacier:ArchiveAgeInDays	
InitiateMultipartUpload	Grants permission to initiate a multipart upload	Write	vault*		
InitiateVaultLock	Grants permission to initiate the vault locking process	Permissions management	vault*		
ListJobs	Grants permission to list jobs for a vault that are in-progress and jobs that have recently finished	List	vault*		
ListMultipartUploads	Grants permission to list in-progress multipart uploads for the specified vault	List	vault*		
ListParts	Grants permission to list the parts of an archive that have been uploaded in a specific multipart upload	List	vault*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListProvisionedCapacity	Grants permission to list the provisioned capacity for the specified Amazon Web Services account	List			
ListTagsForVault	Grants permission to list all the tags attached to a vault	List	vault*		
ListVaults	Grants permission to list all vaults	List			
PurchaseProvisionedCapacity	Grants permission to purchases a provisioned capacity unit for an Amazon Web Services account	Write			
RemoveTagsFromVault	Grants permission to remove one or more tags from the set of tags attached to a vault	Tagging	vault*		
SetDataRetrievalPolicy	Grants permission to set and then enacts a data retrieval policy in the region specified in the PUT request	Permissions management			
SetVaultAccessPolicy	Grants permission to configure an access policy for a vault; will overwrite an existing policy	Permissions management	vault*		
SetVaultNotifications	Grants permission to configure vault notifications	Write	vault*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UploadArchive	Grants permission to upload an archive to a vault	Write	vault*		
UploadMultipartPart	Grants permission to upload a part of an archive	Write	vault*		

Resource types defined by Amazon S3 Glacier

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
vault	`arn:${Partition}:glacier:${Region}:${Account}:vaults/${VaultName}`	

Condition keys for Amazon S3 Glacier

Amazon S3 Glacier 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 Amazon global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by the tags that are passed in the request	String
aws:TagKeys	Filters access by the tag keys that are passed in the request	ArrayOfString
glacier:ArchiveAgeInDays	Filters access by how long an archive has been stored in the vault, in days	String
glacier:ResourceTag/	Filters access by a customer-defined tag	String

Actions, resources, and condition keys for Amazon S3 Object Lambda

Amazon S3 Object Lambda (service prefix: `s3-object-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 Amazon S3 Object Lambda
- Resource types defined by Amazon S3 Object Lambda
- Condition keys for Amazon S3 Object Lambda

Actions defined by Amazon S3 Object 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 Amazon. 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.

> **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	objectlambdaaccesspoint*		
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda: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	objectlambdaaccesspoint*		
				s3-object-lambda:authType s3-object-lambda:s	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ignatureAge s3-object-lambda:TlsVersion	
DeleteObjectTagging	Grants permission to use the tagging subresource to remove the entire tag set from the specified object	Tagging	objectlambdaaccesspoint*		
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
DeleteObjectVersion	Grants permission to remove a specific version of an object	Write	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
DeleteObjectVersionTagging	Grants permission to remove the entire tag set for a specific version of the object	Tagging	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
GetObject	Grants permission to retrieve objects from Amazon S3	Read	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectAcl	Grants permission to return the access control list (ACL) of an object	Read	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectLegalHold	Grants permission to get an object's current Legal Hold status	Read	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectRetention	Grants permission to retrieve the retention settings for an object	Read	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectTagging	Grants permission to return the tag set of an object	Read	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
GetObjectVersion	Grants permission to retrieve a specific version of an object	Read	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
GetObjectVersionAcl	Grants permission to return the access control list (ACL) of a specific object version	Read	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
GetObjectVersionTagging	Grants permission to return the tag set for a specific version of the object	Read	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
ListBucket	Grants permission to list some or all of the objects in an Amazon S3 bucket (up to 1000)	List	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
ListBucketMultipartUploads	Grants permission to list in-progress multipart uploads	List	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
ListBucketVersions	Grants permission to list metadata about all the versions of objects in an Amazon S3 bucket	List	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
ListMultipartUploadParts	Grants permission to list the parts that have been uploaded for a specific multipart upload	List	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObject	Grants permission to add an object to a bucket	Write	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObjectAcl	Grants permission to set the access control list (ACL) permissions for new or existing objects in an S3 bucket	Permissions management	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObjectLegalHold	Grants permission to apply a Legal Hold configuration to the specified object	Write	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObjectRetention	Grants permission to place an Object Retention configuration on an object	Write	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
PutObjectTagging	Grants permission to set the supplied tag-set to an object that already exists in a bucket	Tagging	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
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	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
PutObjectVersionTagging	Grants permission to set the supplied tag-set for a specific version of an object	Tagging	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion s3-object-lambda:versionid	
RestoreObject	Grants permission to restore an archived copy of an object back into Amazon S3	Write	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	
WriteGetObjectResponse	Grants permission to provide data for GetObject requests send to S3 Object Lambda	Write	objectlambdaaccesspoint*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				s3-object-lambda:authType s3-object-lambda:signatureAge s3-object-lambda:TlsVersion	

Resource types defined by Amazon S3 Object 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
objectlambdaaccesspoint	`arn:${Partition}:s3-object-lambda:${Region}:${Account}:accesspoint/${AccessPointName}`	

Condition keys for Amazon S3 Object Lambda

Amazon S3 Object 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 Amazon global condition context keys.

Condition keys	Description	Type
s3-object-lambda:TlsVersion	Filters access by the TLS version used by the client	Numeric
s3-object-lambda:authType	Filters access by authentication method	String
s3-object-lambda:signatureAge	Filters access by the age in milliseconds of the request signature	Numeric
s3-object-lambda:versionid	Filters access by a specific object version	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 Amazon. 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.

> **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-component*		
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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			cluster-scheduler-config		
			code-repository		
			compilation-job		
			compute-quota		
			context		
			data-quality-job-definition		
			device		
			device-fleet		
			domain		
			edge-deployment-plan		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			edge-packaging-job		
			endpoint		
			endpoint-config		
			experiment		
			experiment-trial		
			experiment-trial-component		
			feature-group		
			flow-definition		
			hub		
			hub-content		
			human-task-ui		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			hyper-parameter-tuning-job		
			image		
			inference-component		
			inference-recommendations-job		
			labeling-job		
			mlflow-tracking-server		
			model		
			model-bias-job-definition		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			model-card		
			model-explainability-job-definition		
			model-package		
			model-package-group		
			model-quality-job-definition		
			monitoring-schedule		
			notebook-instance		
			optimization-job		
			partner-app		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			pipeline		
			processing-job		
			project		
			reserved-capacity		
			space		
			studio-lifecycle-config		
			training-job		
			training-plan		
			transform-job		
			user-profile		
			workteam		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys sagemaker:TaggingAction	
AssociateTrialComponent	Grants permission to associate a trial component with a trial	Write	experiment-trial*		
			experiment-trial-component*		
BatchDeleteClusterNodes	Grants permission to batch delete SageMaker HyperPod cluster nodes	Write	cluster*		eks:DescribeCluster
BatchDescribeModelPackage	Grants permission to describe one or more ModelPackages	Read	model-package*		
BatchGetMetrics	Grants permission to retrieve metrics associated with SageMaker Resources such as Training Jobs or Trial Components	Read	experiment-trial-component*		
			training-job*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchGetRecord	Grants permission to get a batch of records from one or more feature groups	Read	feature-group*		
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*		
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	
CreateAppImageConfig	Grants permission to create an AppImageConfig	Write	app-image-config*		sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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*		eks:AssociateAccessPolicy eks:CreateAccessEntry eks:DeleteAccessEntry eks:DescribeAccessEntry eks:DescribeCluster iam:CreateServiceLinkedRole iam:PassRole sagemaker:AddTags
			reserved-capacity		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			training-plan		
				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	
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/${TagKey} aws:TagKeys	
CreateHubContentReference	Grants permission to create hub content reference	Write	hub*		sagemaker:AddTags
			hub-content*		
				aws:RequestTag/${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/${TagKey} aws:TagKeys	
CreateInferenceRecommendationsJob	Grants permission to create an inference recommendations job	Write	inference-recommendations-job*		iam:PassRole sagemaker:AddTags
				aws:RequestTag/${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			
CreateMlflowTrackingServer	Grants permission to create an MLflow tracking server	Write	mlflow-tracking-server*		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: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*		
CreateOptimizationJob	Grants permission to create an optimization job	Write	optimization-job*		iam:PassRole sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreatePartnerApp	Grants permission to create an Amazon SageMaker Partner AI App	Write	partner-app*		sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	
CreatePartnerAppPresignedUrl	Grants permission to return a URL that you can use from your browser to connect to the Amazon SageMaker Partner AI App	Write	partner-app*		
CreatePipeline	Grants permission to create a pipeline	Write	pipeline*		iam:PassRole sagemaker:AddTags
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		
CreatePresignedNotebookInstanceUrl	Grants permission to create a URL that you can use from your browser to connect to the Notebook Instance	Write	notebook-instance*		
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:SpaceSharingType	
CreateStudioLifecycleConfig	Grants permission to create a Studio Lifecycle Configuration that can be deployed using Amazon SageMaker	Write	studio-lifecycle-config*		sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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:EnableRemoteDebug 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	
CreateWorkforce	Grants permission to create a workforce	Write	workforce*		sagemaker:AddTags

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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			
DeleteMlflowTrackingServer	Grants permission to delete an MLflow tracking server	Write	mlflow-tracking-server*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		
DeleteModelPackageGroup	Grants permission to delete a ModelPackageGroup	Write	model-package-group*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteModelPackageGroupPolicy	Grants permission to delete a ModelPackageGroup policy	Write	model-package-group*		
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*		
DeletePartnerApp	Grants permission to delete an Amazon SageMaker Partner AI App	Write	partner-app*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 Amazon 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*		
				sagemaker:OwnerUserProfileArn sagemaker:SpaceSharingType	
DeleteStudioLifecycleConfig	Grants permission to delete a Studio Lifecycle Configuration	Write	studio-lifecycle-config*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
			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-tracking-server		
			model		
			model-bias-job-definition		
			model-card		
			model-explainability-job-definition		
			model-package		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			model-package-group		
			model-quality-job-definition		
			monitoring-schedule		
			notebook-instance		
			optimization-job		
			partner-app		
			pipeline		
			processing-job		
			project		
			reserved-capacity		
			space		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			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*		
DeleteWorkforce	Grants permission to delete a workforce	Write	workforce*		

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
DescribeInferenceExperiment	Grants permission to get information about an inference experiment	Read	inference-experiment*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
DescribeMlflowTrackingServer	Grants permission to get information about an MLflow tracking server	Read	mlflow-tracking-server*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeModelCardExportJob	Grants permission to get information about a model card export job	Read	model-card-export-job*		
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*		
DescribeModelPackageGroup	Grants permission to describe a ModelPackageGroup	Read	model-package-group*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
DescribePartnerApp	Grants permission to describe an Amazon SageMaker Partner AI App	Read	partner-app*		
DescribePipeline	Grants permission to get information about a pipeline	Read	pipeline*		
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
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*		
DescribeTrialComponent	Grants permission to return information about a trial component	Read	experiment-trial-component*		

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
GetResourcePolicy [permission only]	Grants Amazon 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			

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

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

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

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListImages	Grants permission to list SageMaker Images in your account	List			
ListInferenceComponents	Grants permission to list inference components	List			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListMlflowTrackingServers	Grants permission to list MLflow tracking servers	List			
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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListModelQualityJobDefinitions	Grants permission to list model quality job definitions	List			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListNotebookInstances	Grants permission to list the Amazon SageMaker notebook instances in the requester's account in an Amazon Web Services Region	List			
ListOptimizationJobs	Grants permission to list optimization jobs	List			
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*		
ListPipelines	Grants permission to list pipelines	List			
ListProcessingJobs	Grants permission to list processing jobs	List			
ListProjects	Grants permission to list Projects	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListResourceCatalogs	Grants permission to list resource catalogs	List			
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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTags	Grants permission to list the tag set associated with the specified resource	List	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-tracking-server		
			model		
			model-bias-job-definition		
			model-card		
			model-explainability-job-definition		
			model-package		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			model-package-group		
			model-quality-job-definition		
			monitoring-schedule		
			notebook-instance		
			optimization-job		
			partner-app		
			pipeline		
			processing-job		
			project		
			reserved-capacity		
			space		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			studio-lifecycle-config		
			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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTrialComponents	Grants permission to list trial components	List			
ListTrials	Grants permission to list trials	List			
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 Amazon Resource Access Manager permission to create a resource policy on a SageMaker resource that supports cross-account sharing	Write			
QueryLineage	Grants permission to explore the lineage graph	List			

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopMonitoringSchedule	Grants permission to stop a monitoring schedule	Write	monitoring-schedule*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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*		eks:AssociateAccessPolicy eks:CreateAccessEntry eks:DeleteAccessEntry eks:DescribeAccessEntry eks:DescribeCluster iam:PassRole sagemaker:BatchDeleteClusterNodes
			reserved-capacity		
			training-plan		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sagemaker:InstanceTypes sagemaker:VpcSecurityGroupIds sagemaker:VpcSubnets	
UpdateClusterSchedulerConfig	Grants permission to update a cluster scheduler config	Write	cluster-scheduler-config*		
UpdateClusterSoftware	Grants permission to update platform software for a SageMaker HyperPod cluster	Write	cluster*		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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateDevices	Grants permission to update a set of devices	Write	device*		
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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
UpdateMlflowTrackingServer	Grants permission to update an MLflow tracking server	Write	mlflow-tracking-server*		
UpdateModelCard	Grants permission to update a model card	Write	model-card*		
UpdateModelPackage	Grants permission to update a ModelPackage	Write	model-package*		

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*		
UpdatePipeline	Grants permission to update a pipeline	Write	pipeline*		iam:PassRole
UpdatePipelineExecution	Grants permission to update a pipeline execution	Write	pipeline-execution*		
UpdateProject	Grants permission to update a Project	Write	project*		
				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:SpaceSharingType	
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:EnableRemoteDebug	
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	
UpdateWorkforce	Grants permission to update a workforce	Write	workforce*		
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/${TagKey}
edge-deployment-plan	`arn:${Partition}:sagemaker:${Region}:${Account}:edge-deployment/${EdgeDeploymentPlanName}`	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
human-loop	`arn:${Partition}:sagemaker:${Region}:${Account}:human-loop/${HumanLoopName}`	

Resource types	ARN	Condition keys
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}
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}

Resource types	ARN	Condition keys
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}
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}

Resource types	ARN	Condition keys
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/${TagKey}
notebook-instance-lifecycle-config	arn:${Partition}:sagemaker:${Region}:${Account}:notebook-instance-lifecycle-config/${NotebookInstanceLifecycleConfigName}	
code-repository	arn:${Partition}:sagemaker:${Region}:${Account}:code-repository/${CodeRepositoryName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
image	arn:${Partition}:sagemaker:${Region}:${Account}:image/${ImageName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
image-version	arn:${Partition}:sagemaker:${Region}:${Account}:image-version/${ImageName}/${Version}	
algorithm	arn:${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/${TagKey}
training-job	arn:${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}

Resource types	ARN	Condition keys
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}
model-package	arn:${Partition}:sagemaker:${Region}:${Account}:model-package/${ModelPackageName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
model-package-group	arn:${Partition}:sagemaker:${Region}:${Account}:model-package-group/${ModelPackageGroupName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
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}
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}

Resource types	ARN	Condition keys
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}
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}

Resource types	ARN	Condition keys
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}
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}

Resource types	ARN	Condition keys
pipeline	arn:${Partition}:sagemaker:${Region}:${Account}:pipeline/${PipelineName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
pipeline-execution	arn:${Partition}:sagemaker:${Region}:${Account}:pipeline/${PipelineName}/execution/${RandomString}	
artifact	arn:${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}

Resource types	ARN	Condition keys
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/${TagKey}
shared-model	arn:${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/${MlflowTrackingServerName}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}
compute-quota	arn:${Partition}:sagemaker:${Region}:${Account}:compute-quota/${ComputeQuotaId}	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
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}`	aws:ResourceTag/${TagKey} sagemaker:ResourceTag/${TagKey}

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 Amazon 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

Condition keys	Description	Type
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: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
sagemaker:DomainSharingOutputKmsKey	Filters access by the Domain sharing output KMS key associated with the resource in the request	ARN

Condition keys	Description	Type
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
sagemaker:FeatureGroupOnlineStoreKmsKey	Filters access by the online store kms key associated with the feature group resource in the request	ARN

Condition keys	Description	Type
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
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

Condition keys	Description	Type
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
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

Condition keys	Description	Type
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
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: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

Condition keys	Description	Type
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
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 Amazon Savings Plans

Amazon 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 Amazon Savings Plans

- Resource types defined by Amazon Savings Plans
- Condition keys for Amazon Savings Plans

Actions defined by Amazon 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 Amazon. 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.

> **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/${TagKey} aws:TagKeys	
DeleteQueuedSavingsPlan	Grants permission to delete the queued savings plan associated with customers account	Write	savingsplan*		
				aws:ResourceTag/${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}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeSavingsPlansOfferingRates	Grants permission to describe the rates assciated with savings plans offerings	Read			
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	

Resource types defined by Amazon 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 Amazon Savings Plans

Amazon 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 Amazon 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

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by tag-value assoicated with the resource	String
aws:TagKeys	Filters access by the presence of mandatory tags in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Secrets Manager

Amazon 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 Amazon Secrets Manager
- Resource types defined by Amazon Secrets Manager
- Condition keys for Amazon Secrets Manager

Actions defined by Amazon 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 Amazon. 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.

> **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*		

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	
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	
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	
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	
DescribeSecret	Grants permission to retrieve the metadata about a secret, but not the encrypted data	Read	Secret*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

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*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
GetSecretValue		Read	Secret*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Grants permission to retrieve and decrypt the encrypted data			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
ListSecretVersionIds	Grants permission to list the available versions of a secret	Read	Secret*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
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*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:BlockPublicPolicy secretsmanager:SecretPrimaryRegion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutSecretValue	Grants permission to create a new version of the secret with new encrypted data	Write	Secret*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	
RemoveRegionsFromReplication	Grants permission to remove regions from replication	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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Replicate SecretToRegions	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	
RestoreSecret	Grants permission to cancel deletion of a secret	Write	Secret*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

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

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	
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
UntagResource	Grants permission to remove tags from a secret	Tagging	Secret*		
				secretsmanager:SecretId 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
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	
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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ValidateResourcePolicy	Grants permission to validate a resource policy before attaching policy	Permissions management	Secret*		
				secretsmanager:SecretId secretsmanager:resource/AllowRotationLambdaArn secretsmanager:ResourceTag/tag-key aws:ResourceTag/${TagKey} secretsmanager:SecretPrimaryRegion	

Resource types defined by Amazon 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

Condition keys for Amazon Secrets Manager

Amazon 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 Amazon 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

Condition keys	Description	Type
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 Amazon Web Services account access	Bool
secretsmanager:Description	Filters access by the description text in the request	String
secretsmanager:ForceDeleteWithoutRecovery	Filters access by whether the secret is to be deleted immediately without any recovery window	Bool
secretsmanager:ForceOverwriteReplicaSecret	Filters access by whether to overwrite a secret with the same name in the destination Region	Bool
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

Condition keys	Description	Type
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
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	String
secretsmanager:VersionId	Filters access by the unique identifier of the version of the secret in the request	String

Condition keys	Description	Type
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

Actions, resources, and condition keys for Amazon Security Hub

Amazon 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 Amazon Security Hub
- Resource types defined by Amazon Security Hub
- Condition keys for Amazon Security Hub

Actions defined by Amazon 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 Amazon. 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.

> **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		

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

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchUpdateFindings	Grants permission to update customer-controlled fields for a selected set of Security Hub findings	Write	hub		
				securityhub:ASFFSyntaxPath/${ASFFSyntaxPath}	
BatchUpdateStandardsControlAssociations	Grants permission to update the enablement status of a batch of security controls in standards	Write			securityhub:UpdateStandardsControl
CreateActionTarget	Grants permission to create custom actions in Security Hub	Write	hub		
CreateAutomationRule	Grants permission to create an automation rule based on input parameters	Write		aws:RequestTag/${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	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateFindingAggregator	Grants permission to create a finding aggregator, which contains the cross-Region finding aggregation configuration	Write			
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		
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		
DeleteConfigurationPolicy	Grants permission to delete an existing configuration policy	Write	configuration-policy*		
DeleteFindingAggregator	Grants permission to delete a finding aggregator, which disables finding aggregation across Regions	Write	finding-aggregator*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
DescribeProducts	Grants permission to retrieve information about the available Security Hub product integrations	Read	hub		
DescribeStandards	Grants permission to retrieve information about Security Hub standards	Read	hub		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
DisableOrganizationAdminAccount	Grants permission to remove the Security Hub administrator account for your organization	Write	hub		organizations:DescribeOrganization
DisableSecurityHub	Grants permission to disable Security Hub	Write	hub		
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		
DisassociateMembers	Grants permission to disassociate Security Hub member accounts from the associated administrator account	Write	hub		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
EnableImportFindingsForProduct	Grants permission to enable the findings importing for a Security Hub integrated product	Write	hub		
EnableOrganizationAdminAccount	Grants permission to designate a Security Hub administrator account for your organization	Write	hub		organizations:DescribeOrganization organizations:EnableAWSServiceAccess organizations:RegisterDelegatedAdministrator
EnableSecurityHub	Grants permission to enable Security Hub	Write	hub		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAdhocInsightResults [permission only]	Grants permission to retrieve insight results by providing a set of filters instead of an insight ARN	Read	hub		
GetAdministratorAccount	Grants permission to retrieve details about the Security Hub administrator account	Read	hub		
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			
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		
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		
GetInsightResults	Grants permission to retrieve insight results from Security Hub	Read	hub		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
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 Amazon accounts to become Security Hub member accounts	Write	hub		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAutomationRules	Grants permission to retrieve a list of automation rules and their metadata for the calling account from Security Hub	List			
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			
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
ListSecurityControlDefinitions	Grants permission to retrieve a list of security control definitions, which contain details for security controls in the current region	List			
ListStandardsControlAssociations	Grants permission to list the enablement status of a security control in standards	List			securityhub:DescribeStandardsControls

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListTagsForResource	Grants permission to list of tags associated with a resource	Read	automation-rule		
			configuration-policy		
			hub		
SendFindingEvents [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		
StartConfigurationPolicyDisassociation	Grants permission to remove a configuration policy association from 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
TagResource	Grants permission to add tags to a Security Hub resource	Tagging	automation-rule		
			configuration-policy		
			hub		
UntagResource	Grants permission to remove tags from a Security Hub resource	Tagging	automation-rule		
			configuration-policy		
			hub		
UpdateActionTarget	Grants permission to update custom actions in Security Hub	Write	hub		
UpdateConfigurationPolicy	Grants permission to update an existing configuration policy	Write	configuration-policy*		
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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
UpdateStandardsControl	Grants permission to update Security Hub standards controls	Write	hub		

Resource types defined by Amazon 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}
product	`arn:${Partition}:securityhub:${Region}:${Account}:product/${Company}/${ProductId}`	
finding-aggregator	`arn:${Partition}:securityhub:${Region}:${Account}:finding-aggregator/${FindingAggregatorId}`	
automation-rule	`arn:${Partition}:securityhub:${Region}:${Account}:automation-rule/${AutomationRuleId}`	
configuration-policy	`arn:${Partition}:securityhub:${Region}:${Account}:configuration-policy/${ConfigurationPolicyId}`	

Condition keys for Amazon Security Hub

Amazon 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 Amazon 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

Condition keys	Description	Type
aws:ResourceTag/${TagKey}	Filters access by actions based on tag key-value pairs attached to the resource	String
aws:TagKeys	Filters access by actions based on the presence of tag keys in the request	ArrayOfString
securityhub:ASFFSyntaxPath/${ASFFSyntaxPath}	Filters access by the specified fields and values in the request	String
securityhub:TargetAccount	Filters access by the AwsAccountId field that is specified in the request	String

Actions, resources, and condition keys for Amazon Security Token Service

Amazon 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 Amazon Security Token Service
- Resource types defined by Amazon Security Token Service
- Condition keys for Amazon Security Token Service

Actions defined by Amazon 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 Amazon. 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.

> **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 Amazon 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 cognito-identity.amazonaws.com:amr	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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 accounts.google.com:aud accounts.google.com:sub	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				saml:name qualifier 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:eduperson affiliation saml:eduperson assurance saml:eduperson entitlement saml:eduperson nickname saml:eduperson orgdn saml:eduperson orgunitdn saml:eduperson prim	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aryaffiliation saml:eduperson primaryorgunitdn saml:eduperson principalname saml:eduperson scopedaffiliation saml:eduperson targetedid 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 Amazon 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			
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	user		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetServiceBearerToken [permission only]	Grants permission to obtain a STS bearer token for an Amazon root user, IAM role, or an IAM user	Read		sts:AWSServiceName sts:DurationSeconds	
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 Amazon Web Services account or IAM user	Read			
SetContext [permission only]	Grants permission to set context keys on a STS session	Write	role		
			self-session		
				sts:RequestContext/${ContextKey} sts:RequestContextProviders	
SetSourceIdentity [permission only]	Grants permission to set a source identity on a STS session	Write	role		
			user		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				sts:SourceIdentity	
TagSession [permission only]	Grants permission to add tags to a STS session	Tagging	role		
			user		
				aws:TagKeys aws:RequestTag/${TagKey} sts:TransitiveTagKeys saml:aud	

Resource types defined by Amazon 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/${TagKey}
user	`arn:${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}`	

Condition keys for Amazon Security Token Service

Amazon 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 Amazon 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

Condition keys	Description	Type
accounts.google.com:sub	Filters access by the subject of the claim (the Google user ID)	String
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

Condition keys	Description	Type
iam:ResourceTag/${TagKey}	Filters access by the tags that are attached to the role that is being assumed	String
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:eduperson affiliation	Filters access by the eduPerson attribute	ArrayOfString
saml:eduperson assurance	Filters access by the eduPerson attribute	ArrayOfString

Condition keys	Description	Type
saml:eduperson entitlement	Filters access by the eduPerson attribute	ArrayOfString
saml:eduperson nickname	Filters access by the eduPerson attribute	ArrayOfString
saml:eduperson orgdn	Filters access by the eduPerson attribute	String
saml:eduperson orgunitdn	Filters access by the eduPerson attribute	ArrayOfString
saml:eduperson primaryaffiliation	Filters access by the eduPerson attribute	String
saml:eduperson primaryorgunitdn	Filters access by the eduPerson attribute	String
saml:eduperson principalname	Filters access by the eduPerson attribute	String
saml:eduperson scopedaffiliation	Filters access by the eduPerson attribute	ArrayOfString
saml:eduperson targetedid	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

Condition keys	Description	Type
saml:mail	Filters access by the mail attribute	String
saml:name	Filters access by the name attribute	String
saml:name qualifier	Filters access by the hash value of the issuer, account ID, and friendly name	String
saml:organizationStatus	Filters access by the organizationStatus attribute	String
saml:primaryGroupSID	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:x500UniqueIdentifier	Filters access by the uid attribute	String
sts:AWSServiceName	Filters access by the service that is obtaining a bearer token	String
sts:DurationSeconds	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:RequestContext/${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: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 Server Migration Service

Amazon Server Migration Service (service prefix: `sms`) 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 Server Migration Service
- Resource types defined by Amazon Server Migration Service
- Condition keys for Amazon Server Migration Service

Actions defined by Amazon Server Migration 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 Amazon. 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.

> **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
CreateApp	Grants permission to create an application configuration to migrate on-premise application onto Amazon	Write			
CreateReplicationJob	Grants permission to create a job to migrate on-premise server onto Amazon	Write			
DeleteApp	Grants permission to delete an existing application configuration	Write			
DeleteAppLaunchConfiguration	Grants permission to delete launch configuration for an existing application	Write			
DeleteAppReplicationConfiguration	Grants permission to delete replication configuration for an existing application	Write			
DeleteAppValidationConfiguration	Grants permission to delete validation configuration for an existing application	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteReplicationJob	Grants permission to delete an existing job to migrate on-premise server onto Amazon	Write			
DeleteServerCatalog	Grants permission to delete the complete list of on-premise servers gathered into Amazon	Write			
DisassociateConnector	Grants permission to disassociate a connector that has been associated	Write			
GenerateChangeSet	Grants permission to generate a changeSet for the CloudFormation stack of an application	Write			
GenerateTemplate	Grants permission to generate a CloudFormation template for an existing application	Write			
GetApp	Grants permission to get the configuration and statuses for an existing application	Read			
GetAppLaunchConfiguration	Grants permission to get launch configuration for an existing application	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAppReplicationConfiguration	Grants permission to get replication configuration for an existing application	Read			
GetAppValidationConfiguration	Grants permission to get validation configuration for an existing application	Read			
GetAppValidationOutput	Grants permission to get notification sent from application validation script.	Read			
GetConnectors	Grants permission to get all connectors that have been associated	Read			
GetMessages [permission only]	Grants permission to gets messages from Amazon Server Migration Service to Server Migration Connector	Read			
GetReplicationJobs	Grants permission to get all existing jobs to migrate on-premise servers onto Amazon	Read			
GetReplicationRuns	Grants permission to get all runs for an existing job	Read			
GetServers	Grants permission to get all servers that have been imported	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ImportAppCatalog	Grants permission to import application catalog from Amazon Application Discovery Service	Write			
ImportServerCatalog	Grants permission to gather a complete list of on-premise servers	Write			
LaunchApp	Grants permission to create and launch a CloudFormation stack for an existing application	Write			
ListApps	Grants permission to get a list of summaries for existing applications	List			
NotifyAppValidationOutput	Grants permission to send notification for application validation script	Write			
PutAppLaunchConfiguration	Grants permission to create or update launch configuration for an existing application	Write			
PutAppReplicationConfiguration	Grants permission to create or update replication configuration for an existing application	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutAppValidationConfiguration	Grants permission to put validation configuration for an existing application	Write			
SendMessage [permission only]	Grants permission to send message from Server Migration Connector to Amazon Server Migration Service	Write			
StartAppReplication	Grants permission to create and start replication jobs for an existing application	Write			
StartOnDemandAppReplication	Grants permission to start a replication run for an existing application	Write			
StartOnDemandReplicationRun	Grants permission to start a replication run for an existing replication job	Write			
StopAppReplication	Grants permission to stop and delete replication jobs for an existing application	Write			
TerminateApp	Grants permission to terminate the CloudFormation stack for an existing application	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateApp	Grants permission to update an existing application configuration	Write			
UpdateReplicationJob	Grants permission to update an existing job to migrate on-premise server onto Amazon	Write			

Resource types defined by Amazon Server Migration Service

Amazon Server Migration Service does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon Server Migration Service, specify `"Resource": "*"` in your policy.

Condition keys for Amazon Server Migration Service

ServerMigrationService 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 Amazon global condition context keys.

Actions, resources, and condition keys for Amazon Serverless Application Repository

Amazon Serverless Application Repository (service prefix: `serverlessrepo`) 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 Serverless Application Repository
- Resource types defined by Amazon Serverless Application Repository
- Condition keys for Amazon Serverless Application Repository

Actions defined by Amazon Serverless Application Repository

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 Amazon. 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.

> **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, optionally including an Amazon SAM file to create the first application version in the same call	Write			
CreateApplicationVersion	Grants permission to create an application version	Write	applications*		
CreateCloudFormationChangeSet	Grants permission to create an Amazon CloudFormation ChangeSet for the given application	Write	applications*		
				serverlessrepo:applicationType	
CreateCloudFormationTemplate	Grants permission to create an Amazon CloudFormation template	Write	applications*		
				serverlessrepo:applicationType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteApplication	Grants permission to delete the specified application	Write	applications*		
GetApplication	Grants permission to get the specified application	Read	applications*		
				serverlessrepo:applicationType	
GetApplicationPolicy	Grants permission to get the policy for the specified application	Read	applications*		
GetCloudFormationTemplate	Grants permission to get the specified Amazon CloudFormation template	Read	applications*		
ListApplicationDependencies	Grants permission to retrieve the list of applications nested in the containing application	List	applications*		
				serverlessrepo:applicationType	
ListApplicationVersions	Grants permission to list versions for the specified application owned by the requester	List	applications*		
				serverlessrepo:applicationType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListApplications	Grants permission to list applications owned by the requester	List			
PutApplicationPolicy	Grants permission to put the policy for the specified application	Write	applications*		
SearchApplications	Grants permission to get all applications authorized for this user	Read		serverlessrepo:applicationType	
UnshareApplication	Grants permission to unshare the specified application	Write	applications*		
UpdateApplication	Grants permission to update meta-data of the application	Write	applications*		

Resource types defined by Amazon Serverless Application Repository

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
applications	`arn:${Partition}:serverlessrepo:${Region}:${Account}:applications/${ResourceId}`	

Condition keys for Amazon Serverless Application Repository

Amazon Serverless Application Repository 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 Amazon global condition context keys.

Condition keys	Description	Type
serverlessrepo:applicationType	Filters access by application type	String

Actions, resources, and condition keys for Service Quotas

Service Quotas (service prefix: `servicequotas`) 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 Service Quotas

- Resource types defined by Service Quotas
- Condition keys for Service Quotas

Actions defined by Service Quotas

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 Amazon. 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.

> **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
AssociateServiceQuotaTemplate	Grants permission to associate the Service Quotas template with your organization	Write			organizations:DescribeOrganization organizations:EnableAWSServiceAccess
DeleteServiceQuotaIncreaseRequestFromTemplate	Grants permission to remove the specified service quota from the service quota template	Write			organizations:DescribeOrganization
DisassociateServiceQuotaTemplate	Grants permission to disassociate the Service Quotas template from your organization	Write			organizations:DescribeOrganization
GetAWSDefaultServiceQuota	Grants permission to return the details for the specified service quota, including the Amazon default value	Read			
GetAssociationForServiceQuotaTemplate	Grants permission to retrieve the ServiceQuotaTemplateAssociationStatus value, which tells you if the Service	Read			organizations:DescribeOrganization

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Quotas template is associated with an organization				
GetRequestedServiceQuotaChange	Grants permission to retrieve the details for a particular service quota increase request	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetServiceQuota	Grants permission to return the details for the specified service quota, including the applied value	Read			autoscaling:DescribeAccountLimits cloudformation:DescribeAccountLimits dynamodb:DescribeLimits elasticloadbalancing:DescribeAccountLimits iam:GetAccountSummary kinesis:DescribeLimits rds:DescribeAccountAttributes

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					route53:GetAccountLimit
GetServiceQuotaIncreaseRequestFromTemplate	Grants permission to retrieve the details for a service quota increase request from the service quota template	Read			organizations:DescribeOrganization
ListAWSDefaultServiceQuotas	Grants permission to list all default service quotas for the specified Amazon service	Read			
ListRequestedServiceQuotaChangeHistory	Grants permission to request a list of the changes to quotas for a service	Read			
ListRequestedServiceQuotaChangeHistoryByQuota	Grants permission to request a list of the changes to specific service quotas	Read			
ListServiceQuotaIncreaseRequestsInTemplate	Grants permission to return a list of the service quota increase requests from the service quota template	Read			organizations:DescribeOrganization

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListServiceQuotas	Grants permission to list all service quotas for the specified Amazon service, in that account, in that Region	Read			autoscaling:DescribeAccountLimits cloudformation:DescribeAccountLimits dynamodb:DescribeLimits elasticloadbalancing:DescribeAccountLimits iam:GetAccountSummary kinesis:DescribeLimits rds:DescribeAccountAttributes

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					route53:GetAccountLimit
ListServices	Grants permission to list the Amazon services available in Service Quotas	Read			
ListTagsForResource	Grants permission to view the existing tags on a SQ resource	Read			
PutServiceQuotaIncreaseRequestIntoTemplate	Grants permission to define and add a quota to the service quota template	Write	quota		organizations:DescribeOrganization
				servicequotas:service	
RequestServiceQuotaIncrease	Grants permission to submit the request for a service quota increase	Write	quota		
				servicequotas:service	
TagResource	Grants permission to associate a set of tags with an existing SQ resource	Tagging		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagResource	Grants permission to remove a set of tags from a SQ resource, where tags to be removed match a set of customer-supplied tag keys	Tagging		aws:TagKeys	

Resource types defined by Service Quotas

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
quota	`arn:${Partition}:servicequotas:${Region}:${Account}:${ServiceCode}/${QuotaCode}`	

Condition keys for Service Quotas

Service Quotas 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 Amazon 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
servicequotas:service	Filters access by the specified Amazon service	String

Actions, resources, and condition keys for Amazon Signer

Amazon Signer (service prefix: `signer`) 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 Signer
- Resource types defined by Amazon Signer
- Condition keys for Amazon Signer

Actions defined by Amazon Signer

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 Amazon. 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.

> **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
AddProfilePermission	Grants permission to add cross-account permissions to a Signing Profile	Permissions management	signing-profile*		
CancelSigningProfile	Grants permission to change the state of a Signing Profile to CANCELED	Write	signing-profile*		
				signer:ProfileVersion	
DescribeSigningJob	Grants permission to return information about a specific Signing Job	Read	signing-job*		
GetRevocationStatus	Grants permission to query revocation info of signing resources	Read	signing-job*		
			signing-profile*		
GetSigningPlatform	Grants permission to return information about a specific Signing Platform	Read			
GetSigningProfile	Grants permission to return information about a specific Signing Profile	Read	signing-profile*		
				signer:ProfileVersion	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListProfilePermissions	Grants permission to list the cross-account permissions associated with a Signing Profile	Read	signing-profile*		
ListSigningJobs	Grants permission to list all Signing Jobs in your account	List			
ListSigningPlatforms	Grants permission to list all available Signing Platforms	List			
ListSigningProfiles	Grants permission to list all Signing Profiles in your account	List			
ListTagsForResource	Grants permission to list the tags associated with a Signing Profile	Read	signing-profile*		
PutSigningProfile	Grants permission to create a new Signing Profile	Write		aws:RequestTag/${TagKey} aws:TagKeys	
RemoveProfilePermission	Grants permission to remove cross-account permissions from a Signing Profile	Permissions management	signing-profile*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RevokeSignature	Grants permission to change the state of a Signing Job to REVOKED	Write	signing-job*		
				signer:ProfileVersion	
RevokeSigningProfile	Grants permission to change the state of a Signing Profile to REVOKED	Write	signing-profile*		
				signer:ProfileVersion	
SignPayload	Grants permission to initiate a Signing Job on the provided payload	Write	signing-profile*		
				signer:ProfileVersion	
StartSigningJob	Grants permission to initiate a Signing Job on the provided code	Write	signing-profile*		
				signer:ProfileVersion	
TagResource	Grants permission to add one or more tags to a Signing Profile	Tagging	signing-profile*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove one or more tags from a Signing Profile	Tagging	signing-profile*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Resource types defined by Amazon Signer

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
signing-profile	`arn:${Partition}:signer:${Region}:${Account}:/signing-profiles/${ProfileName}`	aws:ResourceTag/${TagKey}
signing-job	`arn:${Partition}:signer:${Region}:${Account}:/signing-jobs/${JobId}`	

Condition keys for Amazon Signer

Amazon Signer 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 Amazon global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by allowed set of values for each of the tags	String
aws:ResourceTag/${TagKey}	Filters access by tag-value associated with the resource	String
aws:TagKeys	Filters access by presence of mandatory tags in the request	ArrayOfString
signer:ProfileVersion	Filters access by version of the Signing Profile	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 Amazon. 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.

> **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 [permission only]	Grants permission to close the workflow execution and record a WorkflowExecutionCanceled event in the history	Write	domain*		
CompleteWorkflowExecution	Grants permission to close the workflow execution and record a WorkflowExecutionCompleted event in the history	Write	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
[permission only]					
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 Amazon 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 Amazon 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 Amazon 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 Amazon 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 SimpleDB

Amazon SimpleDB (service prefix: sdb) 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 SimpleDB
- Resource types defined by Amazon SimpleDB
- Condition keys for Amazon SimpleDB

Actions defined by Amazon SimpleDB

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 Amazon. 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.

> **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
BatchDeleteAttributes	Performs multiple DeleteAttributes operations in a single call, which reduces round trips and latencies	Write	domain*		
BatchPutAttributes	With the BatchPutAttributes operation, you can perform multiple PutAttribute operations in a single call. With the BatchPutAttributes operation, you can perform multiple PutAttribute operations in a single call	Write	domain*		
CreateDomain	The CreateDomain operation creates a new domain	Write	domain*		
DeleteAttributes	Deletes one or more attributes associated with the item	Write	domain*		
DeleteDomain	The DeleteDomain operation deletes a domain	Write	domain*		
DomainMetadata	Returns information about the domain, including when the domain was created, the number of items and	Read	domain*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	attributes, and the size of attribute names and values				
GetAttributes	Returns all of the attributes associated with the item	Read	domain*		
ListDomains	Description for ListDomains	List			
PutAttributes	The PutAttributes operation creates or replaces attributes in an item	Write	domain*		
Select	Description for Select	Read	domain*		

Resource types defined by Amazon SimpleDB

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:${Partition}:sdb:${Region}:${Account}:domain/${DomainName}`	

Condition keys for Amazon SimpleDB

SimpleDB 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 Amazon global condition context keys.

Actions, resources, and condition keys for Amazon Snowball

Amazon Snowball (service prefix: `snowball`) 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 Snowball
- Resource types defined by Amazon Snowball
- Condition keys for Amazon Snowball

Actions defined by Amazon Snowball

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 Amazon. 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.

> **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
CancelCluster	Grants permission to cancel a cluster job	Write			
CancelJob	Grants permission to cancel the specified job	Write			
CreateAddress	Grants permission to create an address for a Snowball to be shipped to	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateCluster	Grants permission to create an empty cluster	Write			
CreateJob	Grants permission to creates a job to import or export data between Amazon S3 and your on-premises data center	Write			
CreateLongTermPricing	Grants permission to creates a LongTermPricingListEntry for allowing customers to add an upfront billing contract for a job	Write			
CreateReturnShippingLabel	Grants permission to create a shipping label that will be used to return the Snow device to Amazon	Write			
DescribeAddress	Grants permission to get specific details about that address in the form of an Address object	Read			
DescribeAddresses	Grants permission to describe a specified number of ADDRESS objects	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeCluster	Grants permission to describe information about a specific cluster including shipping information, cluster status, and other important metadata	Read			
DescribeJob	Grants permission to describe information about a specific job including shipping information, job status, and other important metadata	Read			
DescribeReturnShippingLabel	Grants permission to describe information on the shipping label of a Snow device that is being returned to Amazon	Read			
GetJobManifest	Grants permission to get a link to an Amazon S3 presigned URL for the manifest file associated with the specified JobId value	Read			
GetJobUnlockCode	Grants permission to get the UnlockCode code value for the specified job	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSnowballUsage	Grants permission to get information about the Snowball service limit for your account, and also the number of Snowballs your account has in use	Read			
GetSoftwareUpdates	Grants permission to return an Amazon S3 presigned URL for an update file associated with a specified JobId	Read			
ListClusterJobs	Grants permission to list JobListEntry objects of the specified length	List			
ListClusters	Grants permission to list ClusterListEntry objects of the specified length	List			
ListCompatibleImages	Grants permission to return a list of the different Amazon EC2 Amazon Machine Images (AMIs) that are owned by your Amazon Web Services account that would be supported for use on a Snow device	List			
ListJobs	Grants permission to list JobListEntry objects of the specified length	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListLongTermPricing	Grants permission to list LongTermPricingListEntry objects for the account making the request	Read			
ListPickupLocations	Grants permission to list Address objects where pickup is available, of the specified length	List			
ListServiceVersions	Grants permission to list all supported versions for Snow on-device services	List			
UpdateCluster	Grants permission to update while a cluster's ClusterState value is in the AwaitingQuorum state, you can update some of the information associated with a cluster	Write			
UpdateJob	Grants permission to update while a job's JobState value is New, you can update some of the information associated with a job	Write			
UpdateJobShipmentState	Grants permission to update the state when a the shipment states changes to a different state	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateLongTermPricing	Grants permission to update a specific upfront billing contract for a job	Write			

Resource types defined by Amazon Snowball

Amazon Snowball does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon Snowball, specify `"Resource": "*"` in your policy.

Condition keys for Amazon Snowball

Snowball 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 Amazon global condition context keys.

Actions, resources, and condition keys for Amazon SNS

Amazon SNS (service prefix: `sns`) 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 SNS
- Resource types defined by Amazon SNS
- Condition keys for Amazon SNS

Actions defined by Amazon SNS

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 Amazon. 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.

> **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 add a statement to a topic's access control policy, granting access for the specified Amazon accounts to the specified actions	Permissions management	topic*		
CheckIfPhoneNumberIsOptedOut	Grants permission to accept a phone number and indicate whether the phone holder has opted out of receiving SMS messages from your account	Read			
ConfirmSubscription	Grants permission to verify an endpoint owner's intent to receive messages by validating the token sent to the endpoint by an earlier Subscribe action	Write	topic*		
CreatePlatformApplication	Grants permission to create a platform application object for one of the supported push notification services, such as APNS and GCM, to which devices and mobile apps may register	Write			iam:PassRole
CreatePlatformEndpoint	Grants permission to create an endpoint for a device and mobile app on one of the supported push notification	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	services, such as GCM and APNS				
CreateSMSSandboxPhoneNumber	Grants permission to add a destination phone number and send a one-time password (OTP) to that phone number for an Amazon Web Services account	Write			
CreateTopic	Grants permission to create a topic to which notifications can be published	Write	topic*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteEndpoint	Grants permission to delete the endpoint for a device and mobile app from Amazon SNS	Write			
DeletePlatformApplication	Grants permission to delete a platform application object for one of the supported push notification services, such as APNS and GCM	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteSMSSandboxPhoneNumber	Grants permission to delete an Amazon Web Services account's verified or pending phone number	Write			
DeleteTopic	Grants permission to delete a topic and all its subscriptions	Write	topic*		
GetDataProtectionPolicy	Grants permission to return the data protection policy of the topic	Read	topic*		
GetEndpointAttributes	Grants permission to retrieve the endpoint attributes for a device on one of the supported push notification services, such as GCM and APNS	Read			
GetPlatformApplicationAttributes	Grants permission to retrieve the attributes of the platform application object for the supported push notification services, such as APNS and GCM	Read			
GetSMSAttributes	Grants permission to return the settings for sending SMS messages from your account	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSMSSandboxAccountStatus	Grants permission to retrieve the sandbox status for the calling account in the target region	Read			
GetSubscriptionAttributes	Grants permission to return all of the properties of a subscription	Read			
GetTopicAttributes	Grants permission to return all of the properties of a topic	Read	topic*		
ListEndpointsByPlatformApplication	Grants permission to list the endpoints and endpoint attributes for devices in a supported push notification service, such as GCM and APNS	List			
ListOriginationNumbers	Grants permission to list all origination numbers, and their metadata	List			
ListPhoneNumbersOptedOut	Grants permission to return a list of phone numbers that are opted out, meaning you cannot send SMS messages to them	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListPlatformApplications	Grants permission to list the platform application objects for the supported push notification services, such as APNS and GCM	List			
ListSMSSandboxPhoneNumbers	Grants permission to list the calling account's current pending and verified destination phone numbers	List			
ListSubscriptions	Grants permission to return a list of the requester's subscriptions	List			
ListSubscriptionsByTopic	Grants permission to return a list of the subscriptions to a specific topic	List	topic*		
ListTagsForResource	Grants permission to list all tags added to the specified Amazon SNS topic	Read	topic		
ListTopics	Grants permission to return a list of the requester's topics	List			
OptInPhoneNumber	Grants permission to opt in a phone number that is currently opted out, which enables you to resume sending SMS messages to the number	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
Publish	Grants permission to send a message to all of a topic's subscribed endpoints	Write	topic*		
PutDataProtectionPolicy	Grants permission to allow a topic owner to set the data protection policy	Write	topic*		
RemovePermission	Grants permission to remove a statement from a topic's access control policy	Permissions management	topic*		
SetEndpointAttributes	Grants permission to set the attributes for an endpoint for a device on one of the supported push notification services, such as GCM and APNS	Write			
SetPlatformApplicationAttributes	Grants permission to set the attributes of the platform application object for the supported push notification services, such as APNS and GCM	Write			iam:PassRole
SetSMSAttributes	Grants permission to set the default settings for sending SMS messages and receiving daily SMS usage reports	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SetSubscriptionAttributes	Grants permission to allow a subscription owner to set an attribute of the topic to a new value	Write			
SetTopicAttributes	Grants permission to allow a topic owner to set an attribute of the topic to a new value	Permissions management	topic*		iam:PassRole
Subscribe	Grants permission to prepare to subscribe an endpoint by sending the endpoint a confirmation message	Write	topic*		
				sns:Endpoint sns:Protocol	
TagResource	Grants permission to add tags to the specified Amazon SNS topic	Tagging	topic		
				aws:RequestTag/${TagKey} aws:TagKeys	
Unsubscribe	Grants permission to delete a subscription	Write			
UntagResource	Grants permission to remove tags from the specified Amazon SNS topic	Tagging	topic		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
VerifySMSSandboxPhoneNumber	Grants permission to verify a destination phone number with a one-time password (OTP) for an Amazon Web Services account	Write			

Resource types defined by Amazon SNS

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
topic	`arn:${Partition}:sns:${Region}:${Account}:${TopicName}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon SNS

Amazon SNS 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 Amazon global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by tags from request	String
aws:ResourceTag/${TagKey}	Filters access by tags associated with the resource	String
aws:TagKeys	Filters access by tag keys from request	ArrayOfString
sns:Endpoint	Filters access by the URL, email address, or ARN from a Subscribe request or a previously confirmed subscription	String
sns:Protocol	Filters access by the protocol value from a Subscribe request or a previously confirmed subscription	String

Actions, resources, and condition keys for Amazon SQL Workbench

Amazon SQL Workbench (service prefix: `sqlworkbench`) 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 SQL Workbench
- Resource types defined by Amazon SQL Workbench
- Condition keys for Amazon SQL Workbench

Actions defined by Amazon SQL Workbench

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 Amazon. 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.

> **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
AssociateConnectionWithChart [permission only]	Grants permission to associate connection to a chart	Write	chart*		
			connection*		
AssociateConnectionWithTab [permission only]	Grants permission to associate connection to a tab	Write	connection*		
AssociateNotebookWithTab [permission only]	Grants permission to associate notebook to a tab	Write	notebook*		
AssociateQueryWithTab [permission only]	Grants permission to associate query to a tab	Write	query*		
BatchDeleteFolder [permission only]	Grants permission to delete folders on your account	Write			
BatchGetNotebookCell [permission only]	Grants permission to get notebook cells content on your account	Read	notebook*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateAccount [permission only]	Grants permission to create SQLWorkbench account	Write			
CreateChart [permission only]	Grants permission to create new saved chart on your account	Write	chart*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateConnection [permission only]	Grants permission to create a new connection on your account	Write	connection*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateFolder [permission only]	Grants permission to create folder on your account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateNotebook [permission only]	Grants permission to create a new notebook on your account	Write	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateNotebookCell [permission only]	Grants permission to create a notebook cell on your account	Write	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateNotebookFromVersion [permission only]	Grants permission to create a new notebook from a notebook version on your account	Write	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateNotebookVersion [permission only]	Grants permission to create a notebook version on your account	Write	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateSavedQuery [permission only]	Grants permission to create a new saved query on your account	Write	query*		
				aws:TagKeys aws:RequestTag/${TagKey}	
DeleteChart [permission only]	Grants permission to remove charts on your account	Write	chart*		
DeleteConnection [permission only]	Grants permission to remove connections on your account	Write	connection*		
DeleteNotebook [permission only]	Grants permission to remove notebooks on your account	Write	notebook*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteNotebookCell [permission only]	Grants permission to remove notebooks cells on your account	Write	notebook*		
DeleteNotebookVersion [permission only]	Grants permission to remove notebooks cells on your account	Write	notebook*		
DeleteQCustomContext [permission only]	Grants permission to delete account-wide custom context	Write			
DeleteSavedQuery [permission only]	Grants permission to remove saved queries on your account	Write	query*		
DeleteSqlGenerationContext [permission only]	Grants permission to delete sql generation context	Write			
DeleteTab [permission only]	Grants permission to remove a tab on your account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DriverExecute [permission only]	Grants permission to execute a query in your redshift cluster	Write	connection*		
DuplicateNotebook [permission only]	Grants permission to create a new notebook by duplicating an existing one on your account	Write	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
ExportNotebook [permission only]	Grants permission to export a notebook on your account	Read	notebook*		
GenerateSession [permission only]	Grants permission to generate a new session on your account	Write			
GetAccountInfo [permission only]	Grants permission to get account info	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAccountSettings [permission only]	Grants permission to get account settings	Read			
GetAutocompletionMetadata [permission only]	Grants permission to get database structure metadata for auto-completion	Read			
GetAutocompletionResource [permission only]	Grants permission to get database structure information for auto-completion	Read			
GetChart [permission only]	Grants permission to get charts on your account	Read	chart*		
GetConnection [permission only]	Grants permission to get connections on your account	Read	connection*		
GetNotebook [permission only]	Grants permission to get notebook metadata on your account	Read	notebook*		
GetNotebookVersion [permission only]	Grants permission to get the content of a notebook version on your account	Read	notebook*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetQCustomContext [permission only]	Grants permission to get account-wide custom context	Read			
GetQSqlPromptQuotas [permission only]	Grants permission to get Q generative SQL maximum prompt quotas	Read			
GetQSqlRecommendations [permission only]	Grants permission to get text to SQL recommendations	Read			
GetQueryExecutionHistory [permission only]	Grants permission to get the query execution history on your account	Read			
GetSavedQuery [permission only]	Grants permission to get saved query on your account	Read	query*		
GetSchemaInference [permission only]	Grants permission to get the columns and data types inferred from a file	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSqlGenerationContext [permission only]	Grants permission to get sql generation context	Read			
GetSqlRecommendations [permission only]	Grants permission to get text to SQL recommendations	Read			
GetUserInfo [permission only]	Grants permission to get user info	Read			
GetUserWorkspaceSettings [permission only]	Grants permission to get workspace settings on your account	Read			
ImportNotebook [permission only]	Grants permission to import a notebook on your account	Write	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListConnections [permission only]	Grants permission to list the connections on your account	List			
ListDatabases [permission only]	Grants permission to list databases of your redshift cluster	List			
ListFiles [permission only]	Grants permission to list files and folders	List			
ListNotebookVersions [permission only]	Grants permission to get notebook versions metadata on your account	List	notebook*		
ListNotebooks [permission only]	Grants permission to list the notebooks on your account	List			
ListQueryExecutionHistory [permission only]	Grants permission to list the query execution history on your account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListRedshiftClusters [permission only]	Grants permission to list redshift clusters on your account	List			
ListSampleDatabases [permission only]	Grants permission to list sample databases	Read			
ListSavedQueryVersions [permission only]	Grants permission to list versions of saved query on your account	List	query*		
ListTabs [permission only]	Grants permission to list tabs on your account	List			
ListTaggedResources [permission only]	Grants permission to list tagged resources	Read			
ListTagsForResource [permission only]	Grants permission to list the tags of an sqlworkbench resource	Read	chart		
			connection		
			notebook		
			query		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PassAccountSettings [permission only]	Grants permission to provide account settings with the request	Write			
PutQCustomContext [permission only]	Grants permission to update account-wide custom context	Write			
PutSqlGenerationContext [permission only]	Grants permission to update sql generation context	Write			
PutTab [permission only]	Grants permission to create or update a tab on your account	Write			
PutUserWorkspaceSettings [permission only]	Grants permission to update workspace settings on your account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RestoreNotebookVersion [permission only]	Grants permission to restore a notebook on your account to a version	Write	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
TagResource [permission only]	Grants permission to tag an sqlworkbench resource	Tagging	chart		
			connection		
			notebook		
			query		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource [permission only]	Grants permission to untag an sqlworkbench resource	Tagging	chart		
			connection		
			notebook		
			query		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys	
UpdateAccountConnectionSettings [permission only]	Grants permission to update account-wide connection settings	Write			
UpdateAccountExportSettings [permission only]	Grants permission to update account-wide export settings	Write			
UpdateAccountGeneralSettings [permission only]	Grants permission to update account-wide general settings	Write			
UpdateAccountQSqlSettings [permission only]	Grants permission to update account-wide text to SQL settings	Write			
UpdateChart [permission only]	Grants permission to update a chart on your account	Write	chart*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateConnection [permission only]	Grants permission to update a connection on your account	Write	connection*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateFileFolder [permission only]	Grants permission to move files on your account	Write	chart		
			query		
UpdateFolder [permission only]	Grants permission to update a folder's name and details on your account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateNotebook [permission only]	Grants permission to update a notebook metadata on your account	Write	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateNotebookCellContent [permission only]	Grants permission to update a notebook cell content on your account	Write	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	
UpdateNotebookCellLayout [permission only]	Grants permission to update a notebook cell layout on your account	Write	notebook*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateSavedQuery [permission only]	Grants permission to update a saved query on your account	Write	query*		
				aws:TagKeys aws:RequestTag/${TagKey}	

Resource types defined by Amazon SQL Workbench

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
connection	`arn:${Partition}:sqlworkbench:${Region}:${Account}:connection/${ResourceId}`	aws:ResourceTag/${TagKey}
query	`arn:${Partition}:sqlworkbench:${Region}:${Account}:query/${ResourceId}`	aws:ResourceTag/${TagKey}
chart	`arn:${Partition}:sqlworkbench:${Region}:${Account}:chart/${ResourceId}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
notebook	`arn:${Partition}:sqlworkbench:${Region}:${Account}:notebook/${ResourceId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon SQL Workbench

Amazon SQL Workbench 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 Amazon 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 that are 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 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 Amazon. 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.

> **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 Amazon 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 Step Functions

Amazon 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 Amazon Step Functions
- Resource types defined by Amazon Step Functions
- Condition keys for Amazon Step Functions

Actions defined by Amazon 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 Amazon. 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.

> **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 Amazon 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 Amazon 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 Amazon 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 Amazon 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}:${MapRunId}	
labelled execution	arn:${Partition}:states:${Region}:${Account}:execution:${StateMachineName}/${MapRunLabel}:${ExecutionId}	
labelled express	arn:${Partition}:states:${Region}:${Account}:express:${StateMachineName}/${MapRunLabel}:${ExecutionId}:${ExpressId}	

Condition keys for Amazon Step Functions

Amazon 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 Amazon 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 Amazon Storage Gateway

Amazon 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 Amazon Storage Gateway
- Resource types defined by Amazon Storage Gateway
- Condition keys for Amazon Storage Gateway

Actions defined by Amazon 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 Amazon. 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.

> **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/${TagKey} aws:TagKeys	
AddCache	Grants permission to configure one or more gateway local disks as cache for a cached-volume gateway	Write	gateway*		
AddTagsToResource	Grants permission to add one or more tags to the specified resource	Tagging	cache-report		
			fs-association		
			gateway		
			share		
			tape		
			tapepool		
			volume		
				aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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 Amazon Web Services 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 Amazon Web Services 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 Amazon Web Services 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 Amazon Web Services 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		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			volume		
ListTapePools	Grants permission to list tape pools owned by your Amazon Web Services 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 Amazon 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 Amazon Storage Gateway

Amazon 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 Amazon 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 Amazon Web Services Support

Amazon Web Services 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 Amazon Web Services Support
- Resource types defined by Amazon Web Services Support
- Condition keys for Amazon Web Services Support

Actions defined by Amazon Web Services 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 Amazon. 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.

> **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**
>
> Amazon Web Services 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 Amazon Web Services Management Console.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
AddAttachmentsToSet	Grants permission to add one or more attachments to an Amazon Web Services Support case	Write			
AddCommunicationToCase	Grants permission to add a customer communication to an Amazon Web Services Support case	Write			
CreateCase	Grants permission to creates a new Amazon Web Services Support case	Write			
DescribeAttachment	Grants permission to describe attachment detail	Read			
DescribeCaseAttributes	Grants permission to allow secondary services to read Amazon Web Services Support case attributes.This is an internally managed function	Read			
DescribeCaseOptions	Grants permission to describe the available options for a single Amazon Web Services	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
	Support case. This is an internally managed function				
DescribeCases	Grants permission to list Amazon Web Services Support cases that matches the given inputs	Read			
DescribeCommunication	Grants permission to get a single communication and attachments for a single Amazon Web Services Support case	Read			
DescribeCommunications	Grants permission to list the communications and attachments for one or more Amazon Web Services 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 Amazon Web Services Support cases	Read			
DescribeServices	Grants permission to list Amazon services and categories that applies to each service	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeSeverityLevels	Grants permission to list severity levels that can be assigned to an Amazon Web Services Support case	Read			
DescribeSupportLevel	Grants permission to return the support level for an Amazon 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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeTrustedAdvisorChecks	Grants permission to get a list of all available Trusted Advisor checks, including name, identifier, category and description	Read			
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 Amazon Web Services Support Center. This is an internally managed function	Write			
InitiateChatForCase	Grants permission to initiate a chat on Amazon Web Services Support Center.This is an internally managed function	Write			
PutCaseAttributes	Grants permission to allow secondary services to attach attributes to Amazon Web Services Support cases. This is an internally managed function	Write			
RateCaseCommunication	Grants permission to rate an Amazon Web Services Support case communication	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 Amazon Web Services Support case	Write			
SearchForCases	Grants permission to return a list of Amazon Web Services Support cases that matches the given inputs	Read			
StartInteraction	Grants permission to start a specific interaction to receive personalized troubleshooting assistance for account and technical issues	Write			
UpdateCaseSeverity	Grants permission to update the severity for a single Amazon Web Services Support case. This is an internally managed function	Write			

Resource types defined by Amazon Web Services Support

Amazon Web Services Support does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon Web Services Support, specify `"Resource": "*"` in your policy.

Condition keys for Amazon Web Services 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 Amazon global condition context keys.

Actions, resources, and condition keys for Amazon Systems Manager

Amazon Systems Manager (service prefix: `ssm`) 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 Systems Manager
- Resource types defined by Amazon Systems Manager
- Condition keys for Amazon Systems Manager

Actions defined by Amazon Systems 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 Amazon. 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.

> **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
AddTagsToResource	Grants permission to add or overwrite one or more tags for a specified Amazon resource	Tagging	association		
			automation-execution		
			document		
			instance		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			maintenancewindow		
			managed-instance		
			opsitem		
			opsmetadata		
			parameter		
			patchbaseline		
			task		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
AssociateOpsItemRelatedItem	Grants permission to associate RelatedItem to an OpsItem	Write	opsitem*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CancelCommand	Grants permission to cancel a specified Run Command command	Write			
CancelMaintenanceWindowExecution	Grants permission to cancel an in-progress maintenance window execution	Write	maintenancewindow*		
CreateActivation	Grants permission to create an activation that is used to register on-premises servers and virtual machines (VMs) with Systems Manager	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateAssociation	Grants permission to associate a specified Systems Manager document with specified instances or other targets	Write	association*		
			document*		
			instance		
			managed-instance		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	
CreateAssociationBatch	Grants permission to combine entries for multiple CreateAssociation operations in a single command	Write	document*		
			instance		
			managed-instance		
				aws:ResourceTag/${TagKey} aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateDocument	Grants permission to create a Systems Manager SSM document	Write	document*		iam:PassRole
				aws:RequestTag/${TagKey} aws:TagKeys ssm:DocumentType	
CreateMaintenanceWindow	Grants permission to create a maintenance window	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateOpsItem	Grants permission to create an OpsItem in OpsCenter	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateOpsMetadata	Grants permission to create an OpsMetadata object for an Amazon resource	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreatePatchBaseline	Grants permission to create a patch baseline	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateResourceDataSync	Grants permission to create a resource data sync configuration, which regularly collects inventory data from managed instances and updates the data in an Amazon S3 bucket	Write	resourcedatasync*		
				ssm:SyncType	
DeleteActivation	Grants permission to delete a specified activation for managed instances	Write			
DeleteAssociation	Grants permission to disassociate a specified SSM document from a specified instance	Write	association		
			document		
			instance		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			managed-instance		
				aws:ResourceTag/${TagKey}	
DeleteDocument	Grants permission to delete a specified SSM document and its instance associations	Write	document*		
				ssm:DocumentType	
DeleteInventory	Grants permission to delete a specified custom inventory type, or the data associated with a custom inventory type	Write			
DeleteMaintenanceWindow	Grants permission to delete a specified maintenance window	Write	maintenancewindow*		
DeleteOpsItem	Grants permission to delete an OpsItem	Write	opsitem*		
DeleteOpsMetadata	Grants permission to delete an OpsMetadata object	Write	opsmetadata*		
DeleteParameter	Grants permission to delete a specified SSM parameter	Write	parameter*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
DeleteParameters	Grants permission to delete multiple specified SSM parameters	Write	parameter*		
				aws:ResourceTag/${TagKey}	
DeletePatchBaseline	Grants permission to delete a specified patch baseline	Write	patchbaseline*		
DeleteResourceDataSync	Grants permission to delete a specified resource data sync	Write	resourcedatasync*		
				ssm:SyncType	
DeleteResourcePolicy	Grants permission to delete a Systems Manager resource policy	Permissions management	document		
			opsitemgroup		
			parameter		
DeregisterManagedInstance	Grants permission to deregister a specified on-premises server or virtual machine (VM) from Systems Manager	Write	managed-instance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ssm:resourceTag/tag-key	
DeregisterPatchBaselineForPatchGroup	Grants permission to deregister a specified patch baseline from being the default patch baseline for a specified patch group	Write	patchbaseline*		
DeregisterTargetFromMaintenanceWindow	Grants permission to deregister a specified target from a maintenance window	Write	maintenancewindow*		
			windowtarget*		
DeregisterTaskFromMaintenanceWindow	Grants permission to deregister a specified task from a maintenance window	Write	maintenancewindow*		
			windowtask*		
DescribeActivations	Grants permission to view details about a specified managed instance activation, such as when it was created and the number of instances registered using the activation	Read			
DescribeAssociation	Grants permission to view details about the specified association for a specified instance or target	Read	association		
			document		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance		
			managed-instance		
				aws:ResourceTag/${TagKey}	
DescribeAssociationExecutionTargets	Grants permission to view information about a specified association execution	Read	association*		
				aws:ResourceTag/${TagKey}	
DescribeAssociationExecutions	Grants permission to view all executions for a specified association	Read	association*		
				aws:ResourceTag/${TagKey}	
DescribeAutomationExecutions	Grants permission to view details about all active and terminated Automation executions	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeAutomationStepExecutions	Grants permission to view information about all active and terminated step executions in an Automation workflow	Read	automation-execution*		
DescribeAvailablePatches	Grants permission to view all patches eligible to include in a patch baseline	Read			
DescribeDocument	Grants permission to view details about a specified SSM document	Read	document*		
				ssm:DocumentType	
DescribeDocumentParameters	Grants permission to display information about SSM document parameters in the Systems Manager console (internal Systems Manager action)	Read	document*		
DescribeDocumentPermission	Grants permission to view the permissions for a specified SSM document	Read	document*		
				ssm:DocumentType	
DescribeEffectiveInstanceAssociations	Grants permission to view all current associations for a specified instance	Read	instance*		
			managed-instance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
DescribeEffectivePatchesForPatchBaseline	Grants permission to view details about the patches currently associated with the specified patch baseline (Windows only)	Read	patchbaseline*		
DescribeInstanceAssociationsStatus	Grants permission to view the status of the associations for a specified instance	Read	instance*		
			managed-instance*		
				aws:ResourceTag/${TagKey}	
DescribeInstanceInformation	Grants permission to view details about a specified instance	Read			
DescribeInstancePatchStates	Grants permission to view status details about patches on a specified instance	Read	instance*		
			managed-instance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} ssm:resourceTag/${TagKey}	
DescribeInstancePatchStatesForPatchGroup	Grants permission to describe the high-level patch state for the instances in the specified patch group	Read			
DescribeInstancePatches	Grants permission to view general details about the patches on a specified instance	Read	instance*		
			managed-instance*		
				aws:ResourceTag/${TagKey} ssm:resourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeInstanceProperties	Grants permission to user's Amazon EC2 console to render managed instances' nodes	Read			
DescribeInventoryDeletions	Grants permission to view details about a specified inventory deletion	Read			
DescribeMaintenanceWindowExecutionTaskInvocations	Grants permission to view details of a specified task execution for a maintenance window	List			
DescribeMaintenanceWindowExecutionTasks	Grants permission to view details about the tasks that ran during a specified maintenance window execution	List			
DescribeMaintenanceWindowExecutions	Grants permission to view the executions of a specified maintenance window	List	maintenancewindow*		
DescribeMaintenanceWindowSchedule	Grants permission to view details about upcoming executions of a specified maintenance window	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeMaintenanceWindowTargets	Grants permission to view a list of the targets associated with a specified maintenance window	List	maintenancewindow*		
DescribeMaintenanceWindowTasks	Grants permission to view a list of the tasks associated with a specified maintenance window	List	maintenancewindow*		
DescribeMaintenanceWindows	Grants permission to view information about all or specified maintenance windows	List			
DescribeMaintenanceWindowsForTarget	Grants permission to view information about the maintenance window targets and tasks associated with a specified instance	List			
DescribeOpsItems	Grants permission to view details about specified OpsItems	Read			
DescribeParameters	Grants permission to view details about a specified SSM parameter	List			
DescribePatchBaselines	Grants permission to view information about patch baselines that meet the specified criteria	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribePatchGroupState	Grants permission to view aggregated status details for patches for a specified patch group	List			
DescribePatchGroups	Grants permission to view information about the patch baseline for a specified patch group	List			
DescribePatchProperties	Grants permission to view details of available patches for a specified operating system and patch property	List			
DescribeSessions	Grants permission to view a list of recent Session Manager sessions that meet the specified search criteria	List			
DisassociateOpsItemRelatedItem	Grants permission to disassociate RelatedItem from an OpsItem	Write	opsitem*		
ExecuteAPI	Grants permission to a Systems Manager delegated administrator to view related resource details about OpsItems across multiple Amazon accounts in the Amazon Web Services Management Console	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetAccessToken	Grants permission to return a credentials set to be used with just-in-time node access	Read	opsitem*		
GetAutomationExecution	Grants permission to view details of a specified Automation execution	Read	automation-execution*		
				aws:ResourceTag/${TagKey}	
GetCalendar [permission only]	Grants permission to view details of a specific calendar	Read	document*		
GetCalendarState	Grants permission to view the calendar state for a change calendar or a list of change calendars	Read	document*		
GetCommandInvocation	Grants permission to view details about the command execution of a specified invocation or plugin	Read			
GetConnectionStatus	Grants permission to view the Session Manager connection status for a specified managed instance	Read	instance		
			managed-instance		
			task		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ssm:resourceTag/${TagKey} aws:ResourceTag/${TagKey}	
GetDefaultPatchBaseline	Grants permission to view the current default patch baseline for a specified operating system type	Read	patchbaseline*		
GetDeployablePatchSnapshotForInstance	Grants permission to retrieve the current patch baseline snapshot for a specified instance	Read			
GetDocument	Grants permission to view the contents of a specified SSM document	Read	document*		
				ssm:DocumentCategories ssm:DocumentType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetExecutionPreview	Grants permission to retrieve an existing preview that shows the effects that running a specified Automation runbook would have on the targeted resources	Read			
GetInventory	Grants permission to view instance inventory details per the specified criteria	Read			
GetInventorySchema	Grants permission to view a list of inventory types or attribute names for a specified inventory item type	Read			
GetMaintenanceWindow	Grants permission to view details about a specified maintenance window	Read	maintenancewindow*		
GetMaintenanceWindowExecution	Grants permission to view details about a specified maintenance window execution	Read			
GetMaintenanceWindowExecutionTask	Grants permission to view details about a specified maintenance window execution task	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetMaintenanceWindowExecutionTaskInvocation	Grants permission to view details about a specific maintenance window task running on a specific target	Read			
GetMaintenanceWindowTask	Grants permission to view details about tasks registered with a specified maintenance window	Read	maintenancewindow*		
GetManifest [permission only]	Grants permission to Systems Manager and SSM Agent to determine package installation requirements for an instance (internal Systems Manager call)	Read			
GetOpsItem	Grants permission to view information about a specified OpsItem	Read	opsitem*		
GetOpsMetadata	Grants permission to retrieve an OpsMetadata object	Read	opsmetadata*		
GetOpsSummary	Grants permission to view summary information about OpsItems based on specified filters and aggregators	Read	resourcedatasync*		
GetParameter	Grants permission to view information about a specified parameter	Read	parameter*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
GetParameterHistory	Grants permission to view details and changes for a specified parameter	Read	parameter*		
				aws:ResourceTag/${TagKey}	
GetParameters	Grants permission to view information about multiple specified parameters	Read	parameter*		
				aws:ResourceTag/${TagKey}	
GetParametersByPath	Grants permission to view information about parameters in a specified hierarchy	Read	parameter*		
				ssm:Recursive	
GetPatchBaseline	Grants permission to view information about a specified patch baseline	Read	patchbaseline*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetPatchBaselineForPatchGroup	Grants permission to view the ID of the current patch baseline for a specified patch group	Read			
GetResourcePolicies	Grants permission to retrieve lists of Systems Manager resource policies	List	document		
			opsitemgroup		
			parameter		
GetServiceSetting	Grants permission to view the account-level setting for an Amazon service	Read	servicesetting*		
LabelParameterVersion	Grants permission to apply an identifying label to a specified version of a parameter	Write	parameter*		
				aws:ResourceTag/${TagKey}	
ListAssociationVersions	Grants permission to list versions of the specified association	List	association*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListAssociations	Grants permission to list the associations for a specified SSM document or managed instance	List			
ListCommandInvocations	Grants permission to list information about command invocations sent to a specified instance	List			
ListCommands	Grants permission to list the commands sent to a specified instance	List			
ListComplianceItems	Grants permission to list compliance status for specified resource types on a specified resource	List			
ListComplianceSummaries	Grants permission to list a summary count of compliant and noncompliant resources for a specified compliance type	List			
ListDocumentMetadataHistory	Grants permission to view metadata history about a specified SSM document	List	document*		
				ssm:DocumentType	
ListDocumentVersions	Grants permission to list all versions of a specified document	List	document*		
				ssm:DocumentType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDocuments	Grants permission to view information about a specified SSM document	List			
ListInstanceAssociations	Grants permission to SSM Agent to check for new State Manager associations (internal Systems Manager call)	List	instance		
			managed-instance		
				aws:ResourceTag/${TagKey}	
ListInventoryEntries	Grants permission to view a list of specified inventory types for a specified instance	List			
ListNodes	Grants permission to view details about managed nodes based on specified filters	List	resourcedatasync*		
ListNodesSummary	Grants permission to view summary information about managed nodes based on specified filters and aggregators	List	resourcedatasync*		
ListOpsItemEvents	Grants permission to view details about OpsItemEvents	List			
ListOpsItemRelatedItems	Grants permission to view details about OpsItem RelatedItems	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListOpsMetadata	Grants permission to view a list of OpsMetadata objects	List			
ListResourceComplianceSummaries	Grants permission to list resource-level summary count	List			
ListResourceDataSync	Grants permission to list information about resource data sync configurations in an account	List		ssm:SyncType	
ListTagsForResource	Grants permission to view a list of resource tags for a specified resource	List	association		
			automation-execution		
			document		
			maintenancewindow		
			managed-instance		
			opsitem		
			opsmetadata		
			parameter		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			patchbaseline		
				aws:ResourceTag/${TagKey}	
ModifyDocumentPermission	Grants permission to share a custom SSM document publicly or privately with specified Amazon accounts	Permissions management	document*		
				ssm:DocumentType	
PutCalendar [permission only]	Grants permission to create/edit a specific calendar	Write	document*		
PutComplianceItems	Grants permission to register a compliance type and other compliance details on a specified resource	Write	instance		
			managed-instance		
				ssm:SourceInstanceARN ec2:SourceInstanceARN	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutConfigurePackageResult [permission only]	Grants permission to SSM Agent to generate a report of the results of specific agent requests (internal Systems Manager call)	Read			
PutInventory	Grants permission to add or update inventory items on multiple specified managed instances	Write			
PutParameter	Grants permission to create an SSM parameter	Write	parameter*		
				aws:RequestTag/${TagKey} aws:TagKeys ssm:Overwrite ssm:Policies	
PutResourcePolicy	Grants permission to create or update a Systems Manager resource policy	Permissions management	document		
			opsitemgroup		
			parameter		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterDefaultPatchBaseline	Grants permission to specify the default patch baseline for an operating system type	Write	patchbaseline*		
RegisterManagedInstance	Grants permission to register a Systems Manager Agent	Write		aws:RequestTag/${TagKey} aws:TagKeys	
RegisterPatchBaselineForPatchGroup	Grants permission to specify the default patch baseline for a specified patch group	Write	patchbaseline*		
RegisterTargetWithMaintenanceWindow	Grants permission to register a target with a specified maintenance window	Write	maintenancewindow*		
RegisterTaskWithMaintenanceWindow	Grants permission to register a task with a specified maintenance window	Write	maintenancewindow*		
RemoveTagsFromResource	Grants permission to remove a specified tag key from a specified resource	Tagging	association		
			automation-execution		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			document		
			instance		
			maintenancewindow		
			managed-instance		
			opsitem		
			opsmetadata		
			parameter		
			patchbaseline		
			task		
				aws:ResourceTag/${TagKey} aws:TagKeys	
ResetServiceSetting	Grants permission to reset the service setting for an Amazon Web Services account to the default value	Write	servicesetting*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ResumeSession	Grants permission to reconnect a Session Manager session to a managed instance	Write	session*		
				ssm:resourceTag/aws:ssmmessages:session-id ssm:resourceTag/aws:ssmmessages:target-id	
SendAutomationSignal	Grants permission to send a signal to change the current behavior or status of a specified Automation execution	Write	automation-execution*		
				aws:ResourceTag/${TagKey}	
SendCommand	Grants permission to run commands on one or more specified managed instances	Write	document*		
			bucket		
			instance		
			managed-instance		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} ssm:resourceTag/${TagKey}	
StartAccessRequest	Grants permission to start the workflow for just-in-time node access sessions	Write	instance		
			managed-instance		
				aws:RequestTag/${TagKey} aws:TagKeys	
StartAssociationsOnce	Grants permission to run a specified association manually	Write	association*		
				aws:ResourceTag/${TagKey}	
StartAutomationExecution	Grants permission to initiate the execution of an Automation document	Write	automation-definition*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			document*		
				aws:RequestTag/${TagKey} aws:TagKeys	
StartChangeRequestExecution	Grants permission to initiate the execution of an Automation Change Template document	Write	automation-definition*		
			document*		
				aws:RequestTag/${TagKey} aws:TagKeys ssm:AutoApprove	
StartExecutionPreview	Grants permission to create a preview showing the effects that running a specified Automation runbook would have on the targeted resources	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartSession	Grants permission to initiate a connection to a specified target for a Session Manager session	Write	document		
			instance		
			managed-instance		
			task		
				ssm:SessionDocumentAccessCheck ssm:resourceTag/${TagKey} aws:ResourceTag/${TagKey} ssm:AccessRequestId	
StopAutomationExecution	Grants permission to stop a specified Automation execution that is already in progress	Write	automation-execution*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
Terminate Session	Grants permission to permanently end a Session Manager connection to an instance	Write	session*		
				ssm:resourceTag/aws:ssmmessages:session-id ssm:resourceTag/aws:ssmmessages:target-id	
UnlabelParameterVersion	Grants permission to remove an identifying label from a specified version of a parameter	Write	parameter*		
				aws:ResourceTag/${TagKey}	
UpdateAssociation	Grants permission to update an association and immediately run the association on the specified targets	Write	association*		
			document		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			instance		
			managed-instance		
				aws:ResourceTag/${TagKey}	
UpdateAssociationStatus	Grants permission to update the status of the SSM document associated with a specified instance	Write	document*		
			instance		
			managed-instance		
				ssm:SourceInstanceARN ec2:SourceInstanceARN aws:ResourceTag/${TagKey}	
UpdateDocument	Grants permission to update one or more values for an SSM document	Write	document*		
				ssm:DocumentType	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateDocumentDefaultVersion	Grants permission to change the default version of an SSM document	Write	document*		
				ssm:DocumentType	
UpdateDocumentMetadata	Grants permission to update the metadata of an SSM document	Write	document*		
				ssm:DocumentType	
UpdateInstanceAssociationStatus [permission only]	Grants permission to SSM Agent to update the status of the association that it is currently running (internal Systems Manager call)	Write	association*		
			instance		
			managed-instance		
				ssm:SourceInstanceARN ec2:SourceInstanceARN aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateInstanceInformation	Grants permission to SSM Agent to send a heartbeat signal to the Systems Manager service in the cloud	Write	instance		
			managed-instance		
				ssm:SourceInstanceARN ec2:SourceInstanceARN	
UpdateMaintenanceWindow	Grants permission to update a specified maintenance window	Write	maintenancewindow*		
UpdateMaintenanceWindowTarget	Grants permission to update a specified maintenance window target	Write	maintenancewindow*		
			windowtarget*		
UpdateMaintenanceWindowTask	Grants permission to update a specified maintenance window task	Write	maintenancewindow*		
			windowtask*		
UpdateManagedInstanceRole	Grants permission to assign or change the IAM role assigned to a specified managed instance	Write	iam-role*		
			managed-instance*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				ssm:resourceTag/tag-key	
UpdateOpsItem	Grants permission to edit or change an OpsItem	Write	opsitem*		
UpdateOpsMetadata	Grants permission to update an OpsMetadata object	Write	opsmetadata*		
UpdatePatchBaseline	Grants permission to update a specified patch baseline	Write	patchbaseline*		
UpdateResourceDataSync	Grants permission to update a resource data sync	Write	resourcedatasync*		
				ssm:SyncType	
UpdateServiceSetting	Grants permission to update the service setting for an Amazon Web Services account	Write	servicesetting*		

Resource types defined by Amazon Systems 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.

> **Note**
>
> Some State Manager API parameters have been deprecated. This might lead to unexpected behavior. For more information, see Working with associations using IAM.

Resource types	ARN	Condition keys
association	`arn:${Partition}:ssm:${Region}:${Account}:association/${AssociationId}`	aws:ResourceTag/${TagKey}
automation-execution	`arn:${Partition}:ssm:${Region}:${Account}:automation-execution/${AutomationExecutionId}`	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key
automation-definition	`arn:${Partition}:ssm:${Region}:${Account}:automation-definition/${AutomationDefinitionName}:${VersionId}`	
bucket	`arn:${Partition}:s3:::${BucketName}`	
document	`arn:${Partition}:ssm:${Region}:${Account}:document/${DocumentName}`	aws:ResourceTag/${TagKey} ssm:DocumentCategories ssm:DocumentType ssm:resourceTag/${TagKey}
iam-role	`arn:${Partition}:iam::${Account}:role/${RoleName}`	

Resource types	ARN	Condition keys
instance	arn:${Partition}:ec2:${Region}:${Account}:instance/${InstanceId}	aws:ResourceTag/${TagKey} ssm:resourceTag/${TagKey}
maintenancewindow	arn:${Partition}:ssm:${Region}:${Account}:maintenancewindow/${ResourceId}	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key
managed-instance	arn:${Partition}:ssm:${Region}:${Account}:managed-instance/${InstanceId}	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key
managed-instance-inventory	arn:${Partition}:ssm:${Region}:${Account}:managed-instance-inventory/${InstanceId}	
opsitem	arn:${Partition}:ssm:${Region}:${Account}:opsitem/${ResourceId}	aws:ResourceTag/${TagKey}
opsitemgroup	arn:${Partition}:ssm:${Region}:${Account}:opsitemgroup/default	
opsmetadata	arn:${Partition}:ssm:${Region}:${Account}:opsmetadata/${ResourceId}	aws:ResourceTag/${TagKey} ssm:resourceTag/${TagKey}

Resource types	ARN	Condition keys
parameter	arn:${Partition}:ssm:${Region}:${Account}:parameter/${ParameterNameWithoutLeadingSlash}	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key
patchbaseline	arn:${Partition}:ssm:${Region}:${Account}:patchbaseline/${PatchBaselineIdResourceId}	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key
session	arn:${Partition}:ssm:${Region}:${Account}:session/${SessionId}	ssm:resourceTag/aws:ssmmessages:session-id ssm:resourceTag/aws:ssmmessages:target-id
resourcedatasync	arn:${Partition}:ssm:${Region}:${Account}:resource-data-sync/${SyncName}	
servicesetting	arn:${Partition}:ssm:${Region}:${Account}:servicesetting/${ResourceId}	
windowtarget	arn:${Partition}:ssm:${Region}:${Account}:windowtarget/${WindowTargetId}	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key
windowtask	arn:${Partition}:ssm:${Region}:${Account}:windowtask/${WindowTaskId}	aws:ResourceTag/${TagKey} ssm:resourceTag/tag-key

Resource types	ARN	Condition keys
task	`arn:${Partition}:ecs:${Region}:${Account}:task/${TaskId}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Systems Manager

Amazon Systems 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 Amazon global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by 'Create' requests based on the allowed set of values for a specified tags	String
aws:ResourceTag/${TagKey}	Filters access by based on a tag key-value pair assigned to the Amazon resource	String
aws:TagKeys	Filters access by 'Create' requests based on whether mandatory tags are included in the request	ArrayOfString
ec2:SourceInstanceARN	Filters access by the ARN of the instance from which the request originated	ARN
ssm:AccessRequestId	Filters access by verifying that a user has access to the access request ID specified in the request	String
ssm:AutoApprove	Filters access by verifying that a user has permission to start Change Manager workflows without a review step (with the exception of change freeze events)	Bool

Condition keys	Description	Type
ssm:DocumentCategories	Filters access by verifying that a user has permission to access a document belonging to a specific category enum	ArrayOfString
ssm:DocumentType	Filters access by verifying that a user has permission to access a document belonging to a specific document type. Only available in "aws", "aws-cn", and "aws-us-gov" partitions	String
ssm:Overwrite	Filters access by controling whether Systems Manager parameters can be overwritten	String
ssm:Policies	Filters access by controlling whether an IAM Entity (user or role) can create or update a parameter that includes a parameter policy	String
ssm:Recursive	Filters access by Systems Manager parameters created in a hierarchical structure	String
ssm:SessionDocumentAccessCheck	Filters access by verifying that a user has permission to access either the default Session Manager configuration document or the custom configuration document specified in a request	Bool
ssm:SourceInstanceARN	Filters access by verifying the Amazon Resource Name (ARN) of the Amazon Systems Manager's managed instance from which the request is made. This key is not present when the request comes from the managed instance authenticated with an IAM role associated with EC2 instance profile	ARN
ssm:SyncType	Filters access by verifying that a user also has access to the ResourceDataSync SyncType specified in the request	String
ssm:resourceTag/${TagKey}	Filters access by a tag key-value pair assigned to the Systems Manager resource	String

Condition keys	Description	Type
ssm:resourceTag/aws:ssmmessages:session-id	Filters access by based on a tag key-value pair assigned to the Systems Manager session resource	String
ssm:resourceTag/aws:ssmmessages:target-id	Filters access by based on a tag key-value pair assigned to the Systems Manager session resource	String
ssm:resourceTag/tag-key	Filters access by based on a tag key-value pair assigned to the Systems Manager resource	String

Actions, resources, and condition keys for Amazon Systems Manager GUI Connect

Amazon Systems Manager GUI Connect (service prefix: `ssm-guiconnect`) 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 Systems Manager GUI Connect
- Resource types defined by Amazon Systems Manager GUI Connect
- Condition keys for Amazon Systems Manager GUI Connect

Actions defined by Amazon Systems Manager GUI Connect

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 Amazon. 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.

> **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
CancelConnection [permission only]	Grants permission to terminate a GUI Connect connection	Write			
DeleteConnectionRecordingPreferences	Grants permission to remove GUI Connect connection recording preferences	Write			
GetConnection [permission only]	Grants permission to get the metadata for a GUI Connect connection	Read			
GetConnectionRecordingPreferences	Grants permission to get GUI Connect connection recording preferences	Read			
ListConnections [permission only]	Grants permission to list the metadata for GUI Connect connections	List			
StartConnection [permission only]	Grants permission to start a GUI Connect connection	Write			
UpdateConnectionRecordingPreferences	Grants permission to update GUI Connect connection recording preferences	Write			

Resource types defined by Amazon Systems Manager GUI Connect

Amazon Systems Manager GUI Connect does not support specifying a resource ARN in the `Resource` element of an IAM policy statement. To allow access to Amazon Systems Manager GUI Connect, specify `"Resource": "*"` in your policy.

Condition keys for Amazon Systems Manager GUI Connect

GUI Connect 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 Amazon global condition context keys.

Actions, resources, and condition keys for Amazon Timestream InfluxDB

Amazon Timestream InfluxDB (service prefix: `timestream-influxdb`) 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 Timestream InfluxDB
- Resource types defined by Amazon Timestream InfluxDB
- Condition keys for Amazon Timestream InfluxDB

Actions defined by Amazon Timestream InfluxDB

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 Amazon. 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.

> **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
CreateDbCluster	Grants permission to create a new Timestream InfluxDB Cluster	Write	db-parame		timestream-influxd

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			ter-group		b:CreateDbInstance
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDbInstance	Grants permission to create a new Timestream InfluxDB instance	Write	db-parameter-group		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateDbParameterGroup	Grants permission to create a new Timestream InfluxDB parameter group	Write		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteDbCluster	Grants permission to delete a Timestream InfluxDB Cluster	Write	db-cluster*		timestream-influxdb:DeleteDbInstance
DeleteDbInstance	Grants permission to delete a Timestream InfluxDB instance	Write	db-instance*		
GetDbCluster	Grants permission to get information about a Timestream InfluxDB Cluster	Read	db-cluster*		
GetDbInstance	Grants permission to get information about a Timestream InfluxDB instance	Read	db-instance*		
GetDbParameterGroup	Grants permission to get information about a Timestream InfluxDB parameter group	Read	db-parameter-group*		
ListDbClusters	Grants permission to list information about all Timestream InfluxDB clusters in the account	List			
ListDbInstances	Grants permission to list information about all Timestream InfluxDB instances in the account	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListDbInstancesForCluster	Grants permission to list information about all Timestream InfluxDB Instances belonging to a cluster	Read	db-cluster*		
ListDbParameterGroups	Grants permission to list information about all Timestream InfluxDB parameter groups	List			
ListTagsForResource	Grants permission to list tags for a Timestream InfluxDB resource	Read	db-cluster		
			db-instance		
			db-parameter-group		
				aws:ResourceTag/${TagKey}	
TagResource	Grants permission to tag a Timestream InfluxDB resource	Tagging	db-cluster		
			db-instance		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			db-parameter-group		
				aws:RequestTag/${TagKey} aws:ResourceTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to untag a Timestream InfluxDB resource	Tagging	db-cluster		
			db-instance		
			db-parameter-group		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey} aws:TagKeys	
UpdateDbCluster	Grants permission to update a Timestream InfluxDB Cluster	Write	db-cluster*		timestream-influxdb:UpdateDbInstance
			db-parameter-group		
UpdateDbInstance	Grants permission to update a Timestream InfluxDB instance	Write	db-instance*		
			db-parameter-group		

Resource types defined by Amazon Timestream InfluxDB

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
db-cluster	`arn:${Partition}:timestream-influxdb:${Region}:${Account}:db-cluster/${DbClusterId}`	aws:ResourceTag/${TagKey}
db-instance	`arn:${Partition}:timestream-influxdb:${Region}:${Account}:db-instance/${DbInstanceIdentifier}`	aws:ResourceTag/${TagKey}
db-parameter-group	`arn:${Partition}:timestream-influxdb:${Region}:${Account}:db-parameter-group/${DbParameterGroupIdentifier}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon Timestream InfluxDB

Amazon Timestream InfluxDB 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 Amazon 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

Condition keys	Description	Type
aws:TagKeys	Filters access by a list of tag keys that are allowed in the request	ArrayOfString

Actions, resources, and condition keys for Amazon Transcribe

Amazon Transcribe (service prefix: `transcribe`) 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 Transcribe
- Resource types defined by Amazon Transcribe
- Condition keys for Amazon Transcribe

Actions defined by Amazon Transcribe

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 Amazon. 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.

> **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
CreateCallAnalyticsCategory	Grants permission to create an analytics category. Amazon Transcribe applies the conditions specified by your analytics categories to your call analytics jobs	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateLanguageModel	Grants permission to create a new custom language model	Write		aws:RequestTag/	s3:GetObject

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey} aws:TagKeys	s3:ListBucket
CreateMedicalVocabulary	Grants permission to create a new custom vocabulary that you can use to change the way Amazon Transcribe Medical handles transcription of an audio file	Write		aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
CreateVocabulary	Grants permission to create a new custom vocabulary that you can use to change the way Amazon Transcribe handles transcription of an audio file	Write		aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
CreateVocabularyFilter	Grants permission to create a new vocabulary filter that you can use to filter out words from the transcription of an audio file generated by Amazon Transcribe	Write		aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
DeleteCallAnalyticsCategory	Grants permission to delete a call analytics category using its name from Amazon Transcribe	Write	callanalyticscategory*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteCallAnalyticsJob	Grants permission to delete a previously submitted call analytics job along with any other generated results such as the transcription, models, and so on	Write	callanalyticsjob*		
DeleteLanguageModel	Grants permission to delete a previously created custom language model	Write	languagemodel*		
DeleteMedicalScribeJob	Grants permission to delete a previously submitted Medical Scribe job	Write	medicalscribejob*		
DeleteMedicalTranscriptionJob	Grants permission to delete a previously submitted medical transcription job	Write	medicaltranscriptionjob*		
DeleteMedicalVocabulary	Grants permission to delete a medical vocabulary from Amazon Transcribe	Write	medicalvocabulary*		
DeleteTranscriptionJob	Grants permission to delete a previously submitted transcription job along with any other generated results such as the transcription, models, and so on	Write	transcriptionjob*		
DeleteVocabulary	Grants permission to delete a vocabulary from Amazon Transcribe	Write	vocabulary*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteVocabularyFilter	Grants permission to delete a vocabulary filter from Amazon Transcribe	Write	vocabularyfilter*		
DescribeLanguageModel	Grants permission to return information about a custom language model	Read	languagemodel*		
GetCallAnalyticsCategory	Grants permission to retrieve information about a call analytics category	Read	callanalyticscategory*		
GetCallAnalyticsJob	Grants permission to return information about a call analytics job	Read	callanalyticsjob*		
GetMedicalScribeJob	Grants permission to return information about a Medical Scribe job	Read	medicalscribejob*		
GetMedicalScribeStream	Grants permission to get information about the specified Amazon HealthScribe streaming session	Read			
GetMedicalTranscriptionJob	Grants permission to return information about a medical transcription job	Read	medicaltranscriptionjob*		
GetMedicalVocabulary	Grants permission to get information about a medical vocabulary	Read	medicalvocabulary*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetTranscriptionJob	Grants permission to return information about a transcription job	Read	transcriptionjob*		
GetVocabulary	Grants permission to to get information about a vocabulary	Read	vocabulary*		
GetVocabularyFilter	Grants permission to get information about a vocabulary filter	Read	vocabularyfilter*		
ListCallAnalyticsCategories	Grants permission to list call analytics categories that has been created	List			
ListCallAnalyticsJobs	Grants permission to list call analytics jobs with the specified status	List			
ListLanguageModels	Grants permission to list custom language models	List			
ListMedicalScribeJobs	Grants permission to list Medical Scribe jobs with the specified status	List			
ListMedicalTranscriptionJobs	Grants permission to list medical transcription jobs with the specified status	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListMedicalVocabularies	Grants permission to return a list of medical vocabularies that match the specified criteria. If no criteria are specified, returns the entire list of vocabularies	List			
ListTagsForResource	Grants permission to list tags for a resource	Read			
ListTranscriptionJobs	Grants permission to list transcription jobs with the specified status	List			
ListVocabularies	Grants permission to return a list of vocabularies that match the specified criteria. If no criteria are specified, returns the entire list of vocabularies	List			
ListVocabularyFilters	Grants permission to return a list of vocabulary filters that match the specified criteria. If no criteria are specified, returns the at most 5 vocabulary filters	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartCallAnalyticsJob	Grants permission to start an asynchronous analytics job that not only transcribes the audio recording of a caller and agent, but also returns additional insights	Write		transcribe:OutputEncryptionKMSKeyId transcribe:OutputLocation aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
StartCallAnalyticsStreamTranscription	Grants permission to start a protocol where audio is streamed to Transcribe Call Analytics and the transcription results are streamed to your application	Write			
StartCallAnalyticsStreamTranscriptionWebSocket	Grants permission to start a WebSocket where audio is streamed to Transcribe Call Analytics and the transcription results are streamed to your application	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartMedicalScribeJob	Grants permission to start an asynchronous job to transcribe patient-clinician conversations and generates clinical notes	Write		transcribe:OutputBucketName transcribe:OutputEncryptionKMSKeyId aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
StartMedicalScribeStream	Grants permission to start a bidirectional HTTP2 stream where audio is streamed to Amazon HealthScribe and the transcription results are streamed to your application	Write			
StartMedicalStreamTranscription	Grants permission to start a protocol where audio is streamed to Transcribe Medical and the transcription results are streamed to your application	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartMedicalStreamTranscriptionWebSocket	Grants permission to start a WebSocket where audio is streamed to Transcribe Medical and the transcription results are streamed to your application	Write			
StartMedicalTranscriptionJob	Grants permission to start an asynchronous job to transcribe medical speech to text	Write		transcribe:OutputBucketName transcribe:OutputEncryptionKMSKeyId transcribe:OutputKey aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
StartStreamTranscription	Grants permission to start a bidirectional HTTP2 stream to transcribe speech to text in real time	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StartStreamTranscriptionWebSocket	Grants permission to start a websocket stream to transcribe speech to text in real time	Write			
StartTranscriptionJob	Grants permission to start an asynchronous job to transcribe speech to text	Write		transcribe:OutputBucketName transcribe:OutputEncryptionKMSKeyId transcribe:OutputKey aws:RequestTag/${TagKey} aws:TagKeys	s3:GetObject
TagResource	Grants permission to tag a resource with given key value pairs	Tagging		aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UntagResource	Grants permission to untag a resource with given key	Tagging		aws:TagKeys	
UpdateCallAnalyticsCategory	Grants permission to update the call analytics category with new values. The UpdateCallAnalyticsCategory operation overwrites all of the existing information with the values that you provide in the request	Write	callanalyticscategory*		
UpdateMedicalVocabulary	Grants permission to update an existing medical vocabulary with new values. The UpdateMedicalVocabulary operation overwrites all of the existing information with the values that you provide in the request	Write	medicalvocabulary*		s3:GetObject
UpdateVocabulary	Grants permission to update an existing vocabulary with new values. The UpdateVocabulary operation overwrites all of the existing information with the values that you provide in the request	Write	vocabulary*		s3:GetObject

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateVocabularyFilter	Grants permission to update an existing vocabulary filter with new values. The UpdateVocabularyFilter operation overwrites all of the existing information with the values that you provide in the request	Write	vocabularyfilter*		s3:GetObject

Resource types defined by Amazon Transcribe

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
transcriptionjob	`arn:${Partition}:transcribe:${Region}:${Account}:transcription-job/${JobName}`	aws:ResourceTag/${TagKey}
vocabulary	`arn:${Partition}:transcribe:${Region}:${Account}:vocabulary/${VocabularyName}`	aws:ResourceTag/${TagKey}
vocabularyfilter	`arn:${Partition}:transcribe:${Region}:${Account}:vocabulary-filter/${VocabularyFilterName}`	aws:ResourceTag/${TagKey}

Resource types	ARN	Condition keys
languagemodel	arn:${Partition}:transcribe:${Region}:${Account}:language-model/${ModelName}	aws:ResourceTag/${TagKey}
medicaltranscriptionjob	arn:${Partition}:transcribe:${Region}:${Account}:medical-transcription-job/${JobName}	aws:ResourceTag/${TagKey}
medicalvocabulary	arn:${Partition}:transcribe:${Region}:${Account}:medical-vocabulary/${VocabularyName}	aws:ResourceTag/${TagKey}
callanalyticsjob	arn:${Partition}:transcribe:${Region}:${Account}:analytics/${JobName}	aws:ResourceTag/${TagKey}
callanalyticscategory	arn:${Partition}:transcribe:${Region}:${Account}:analytics-category/${CategoryName}	aws:ResourceTag/${TagKey}
medicalscribejob	arn:${Partition}:transcribe:${Region}:${Account}:medical-scribe-job/${JobName}	aws:ResourceTag/${TagKey}

Condition keys for Amazon Transcribe

Amazon Transcribe 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 Amazon global condition context keys.

Condition keys	Description	Type
aws:RequestTag/${TagKey}	Filters access by requiring tag values present in a resource creation request	String
aws:ResourceTag/${TagKey}	Filters access by requiring tag value associated with the resource	String
aws:TagKeys	Filters access by requiring the presence of mandatory tags in the request	ArrayOfString
transcribe:OutputBucketName	Filters access based on the output bucket name included in the request	String
transcribe:OutputEncryptionKMSKeyId	Filters access based on the KMS key id included in the request	String
transcribe:OutputKey	Filters access based on the output key included in the request	String
transcribe:OutputLocation	Filters access based on the output location included in the request	String

Actions, resources, and condition keys for Amazon Transfer Family

Amazon 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 Amazon Transfer Family
- Resource types defined by Amazon Transfer Family
- Condition keys for Amazon Transfer Family

Actions defined by Amazon 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 Amazon. 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.

> **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 aws:RequestTag/${TagKey}	
CreateConnector	Grants permission to create a connector	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:PassRole
CreateProfile	Grants permission to create a profile	Write		aws:TagKeys aws:RequestTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey}	
CreateServer	Grants permission to create a server	Write		aws:TagKeys aws:RequestTag/${TagKey}	iam:PassRole
CreateUser	Grants permission to add a user associated with a server	Write	server*		iam:PassRole
				aws:TagKeys aws:RequestTag/${TagKey}	
CreateWebApp	Grants permission to create a webapp	Write		aws:TagKeys aws:RequestTag/${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}	
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*		
DeleteSshPublicKey	Grants permission to delete an SSH public key from a user	Write	user*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
DescribeHostKey	Grants permission to describe a host key associated with a server	Read	host-key*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
ImportCertificate	Grants permission to add a certificate	Write		aws:TagKeys aws:RequestTag/${TagKey}	
ImportHostKey	Grants permission to add a host key to a server	Write	server*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:TagKeys aws:RequestTag/${TagKey}	
ImportSshPublicKey	Grants permission to add an SSH public key to a user	Write	user*		
ListAccesses	Grants permission to list accesses	Read	server*		
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*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 Amazon Transfer Family resource	Read	agreement		
			certificate		
			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			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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*		
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 Amazon Transfer Family resource	Tagging	agreement		
			certificate		
			connector		
			host-key		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			profile		
			server		
			user		
			webapp		
			workflow		
				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 Amazon Transfer Family resource	Tagging	agreement		
			certificate		
			connector		
			host-key		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			profile		
			server		
			user		
			webapp		
			workflow		
				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

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 Amazon 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 Amazon Transfer Family

Amazon 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 Amazon 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

Actions, resources, and condition keys for Amazon Trusted Advisor

Amazon Trusted Advisor (service prefix: `trustedadvisor`) 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 Trusted Advisor
- Resource types defined by Amazon Trusted Advisor
- Condition keys for Amazon Trusted Advisor

Actions defined by Amazon Trusted Advisor

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 Amazon. 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.

> **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 IAM Trusted Advisor policy description details apply only to the Trusted Advisor console. If you want to manage programmatic access to Trusted Advisor, use the Trusted Advisor operations in the Amazon Web Services Support API.

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
BatchUpdateRecommendationResourceExclusion	Grants permission to update one or more exclusion status for a list of recommendation resources	Write			
CreateEngagement	Grants permission to create an engagement	Write			
CreateEngagementAttachment	Grants permission to create an engagement attachment	Write			
CreateEngagementCommunication	Grants permission to create an engagement communication	Write			
DeleteNotificationConfigurationForDelegatedAdmin	Grants permission to the organization management account to delete email notification preferences from a delegated administrator account for Trusted Advisor Priority	Write			
DescribeAccount [permission only]	Grants permission to view the Amazon Web Services Support plan and various Amazon Trusted Advisor preferences	Read			
DescribeAccountAccess	Grants permission to view if the Amazon Web Services	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
[permission only]	account has enabled or disabled Amazon Trusted Advisor				
DescribeCheckItems	Grants permission to view details for the check items	Read	checks*		
DescribeCheckRefreshStatuses	Grants permission to view the refresh statuses for Amazon Trusted Advisor checks	Read	checks*		
DescribeCheckStatusHistoryChanges [permission only]	Grants permission to view the results and changed statuses for checks in the last 30 days	Read	checks*		
DescribeCheckSummaries	Grants permission to view Amazon Trusted Advisor check summaries	Read	checks*		
DescribeChecks	Grants permission to view details for Amazon Trusted Advisor checks	Read			
DescribeNotificationConfigurations	Grants permission to get your email notification preferences for Trusted Advisor Priority	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeNotificationPreferences [permission only]	Grants permission to view the notification preferences for the Amazon Web Services account	Read			
DescribeOrganization [permission only]	Grants permission to view if the Amazon Web Services account meets the requirements to enable the organizational view feature	Read			
DescribeOrganizationAccounts [permission only]	Grants permission to view the linked Amazon accounts that are in the organization	Read			
DescribeReports [permission only]	Grants permission to view details for organizational view reports, such as the report name, runtime, date created, status, and format	Read			
DescribeRisk	Grants permission to view risk details in Amazon Trusted Advisor Priority	Read			
DescribeRiskResources	Grants permission to view affected resources for a risk in Amazon Trusted Advisor Priority	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeRisks	Grants permission to view risks in Amazon Trusted Advisor Priority	Read			
DescribeServiceMetadata [permission only]	Grants permission to view information about organizational view reports, such as the Amazon Web Services Regions, check categories, check names, and resource statuses	Read			
DownloadRisk	Grants permission to download a file that contains details about the risk in Amazon Trusted Advisor Priority	Read			
ExcludeCheckItems [permission only]	Grants permission to exclude recommendations for Amazon Trusted Advisor checks	Write	checks*		
GenerateReport [permission only]	Grants permission to create a report for Amazon Trusted Advisor checks in your organization	Write			
GetEngagement	Grants permission to view an engagment	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetEngagementAttachment	Grants permission to view an engagment attachment	Read			
GetEngagementType	Grants permission to view a specific engagement type	Read			
GetOrganizationRecommendation	Grants permission to get a specific recommendation within an Amazon Organization's organization. This API supports only prioritized recommendations	Read			
GetRecommendation	Grants permission to get a specific Recommendation	Read			
IncludeCheckItems [permission only]	Grants permission to include recommendations for Amazon Trusted Advisor checks	Write	checks*		
ListAccountsForParent [permission only]	Grants permission to view, in the Trusted Advisor console, all of the accounts in an Amazon organization that are contained by a root or organizational unit (OU)	Read			
ListChecks	Grants permission to list a filterable set of Checks	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListEngagementCommunications	Grants permission to view all communications for an engagement	Read			
ListEngagementTypes	Grants permission to view all engagement types	Read			
ListEngagements	Grants permission to view all engagements	Read			
ListOrganizationRecommendationAccounts	Grants permission to list the accounts that own the resources for an Amazon Organization aggregate recommendation. This API only supports prioritized recommendations	List			
ListOrganizationRecommendationResources	Grants permission to list Resources of a Recommendation within an Amazon Organization. This API only supports prioritized recommendations	List			
ListOrganizationRecommendations	Grants permission to list a filterable set of Recommendations within an Amazon Organization. This API only supports prioritized recommendations	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListOrganizationalUnitsForParent [permission only]	Grants permission to view, in the Trusted Advisor console, all of the organizational units (OUs) in a parent organizational unit or root	Read			
ListRecommendationResources	Grants permission to list Resources of a Recommendation	List			
ListRecommendations	Grants permission to list a filterable set of Recommendations	List			
ListRoots [permission only]	Grants permission to view, in the Trusted Advisor console, all of the roots that are defined in an Amazon organization	Read			
RefreshCheck	Grants permission to refresh an Amazon Trusted Advisor check	Write	checks*		
SetAccountAccess [permission only]	Grants permission to enable or disable Amazon Trusted Advisor for the account	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
SetOrganizationAccess [permission only]	Grants permission to enable the organizational view feature for Amazon Trusted Advisor	Write			
UpdateEngagement	Grants permission to update the details of an engagement	Write			
UpdateEngagementStatus	Grants permission to update the status of an engagement	Write			
UpdateNotificationConfigurations	Grants permission to create or update your email notification preferences for Trusted Advisor Priority	Write			
UpdateNotificationPreferences [permission only]	Grants permission to update notification preferences for Amazon Trusted Advisor	Write			
UpdateOrganizationRecommendationLifecycle	Grants permission to update the lifecyle of a Recommendation within an Amazon Organization. This API only supports prioritized recommendations	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateRecommendationLifecycle	Grants permission to update the lifecycle of a Recommendation. This API only supports prioritized recommendations	Write			
UpdateRiskStatus	Grants permission to update the risk status in Amazon Trusted Advisor Priority	Write			

Resource types defined by Amazon Trusted Advisor

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 for the checks resource type should not include a region. In the format instead of '${Region}' use a '*' or the policy will not work correctly.

Resource types	ARN	Condition keys
checks	`arn:${Partition}:trustedadvisor:${Region}:${Account}:checks/${CategoryCode}/${CheckId}`	

Condition keys for Amazon Trusted Advisor

Trusted Advisor 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 Amazon global condition context keys.

Actions, resources, and condition keys for Amazon WAF Regional

Amazon WAF Regional (service prefix: `waf-regional`) 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 WAF Regional
- Resource types defined by Amazon WAF Regional
- Condition keys for Amazon WAF Regional

Actions defined by Amazon WAF Regional

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 Amazon. 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.

> **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
AssociateWebACL	Grants permission to associate a web ACL with a resource	Write	loadbalancer/app/*		
			webacl*		
CreateByteMatchSet	Grants permission to create a ByteMatchSet	Write	bytematchset*		
CreateGeoMatchSet	Grants permission to create a GeoMatchSet	Write	geomatchset*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateIPSet	Grants permission to create an IPSet	Write	ipset*		
CreateRateBasedRule	Grants permission to create a RateBasedRule	Write	ratebasedrule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRegexMatchSet	Grants permission to create a RegexMatchSet	Write	regexmatchset*		
CreateRegexPatternSet	Grants permission to create a RegexPatternSet	Write	regexpatternset*		
CreateRule	Grants permission to create a Rule	Write	rule*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateRuleGroup	Grants permission to create a RuleGroup	Write	rulegroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateSizeConstraintSet	Grants permission to create a SizeConstraintSet	Write	sizeconstraintset*		
CreateSqlInjectionMatchSet	Grants permission to create an SqlInjectionMatchSet	Write	sqlinjectionmatchset*		
CreateWebACL	Grants permission to create a WebACL	Permissions management	webacl*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWebACLMigrationStack	Grants permission to create a CloudFormation web ACL template in an S3 bucket for the purposes of migrating the web ACL from Amazon WAF Classic to Amazon WAF v2	Write	webacl*		s3:PutObject

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateXssMatchSet	Grants permission to create an XssMatchSet	Write	xssmatchset*		
DeleteByteMatchSet	Grants permission to delete a ByteMatchSet	Write	bytematchset*		
DeleteGeoMatchSet	Grants permission to delete a GeoMatchSet	Write	geomatchset*		
DeleteIPSet	Grants permission to delete an IPSet	Write	ipset*		
DeleteLoggingConfiguration	Grants permission to delete a LoggingConfiguration from a web ACL	Write	webacl*		
DeletePermissionPolicy	Grants permission to delete an IAM policy from a rule group	Permissions management	rulegroup*		
DeleteRateBasedRule	Grants permission to delete a RateBasedRule	Write	ratebasedrule*		
DeleteRegexMatchSet	Grants permission to delete a RegexMatchSet	Write	regexmatchset*		
DeleteRegexPatternSet	Grants permission to delete a RegexPatternSet	Write	regexpatternset*		
DeleteRule	Grants permission to delete a Rule	Write	rule*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteRuleGroup	Grants permission to delete a RuleGroup	Write	rulegroup*		
DeleteSizeConstraintSet	Grants permission to delete a SizeConstraintSet	Write	sizeconstraintset*		
DeleteSqlInjectionMatchSet	Grants permission to delete an SqlInjectionMatchSet	Write	sqlinjectionmatchset*		
DeleteWebACL	Grants permission to delete a WebACL	Permissions management	webacl*		
DeleteXssMatchSet	Grants permission to delete an XssMatchSet	Write	xssmatchset*		
DisassociateWebACL	Grants permission to delete an association between a web ACL and a resource	Write	loadbalancer/app/*		
GetByteMatchSet	Grants permission to retrieve a ByteMatchSet	Read	bytematchset*		
GetChangeToken	Grants permission to retrieve a change token to use in create, update, and delete requests	Read			
GetChangeTokenStatus	Grants permission to retrieve the status of a change token	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetGeoMatchSet	Grants permission to retrieve a GeoMatchSet	Read	geomatchset*		
GetIPSet	Grants permission to retrieve an IPSet	Read	ipset*		
GetLoggingConfiguration	Grants permission to retrieve a LoggingConfiguration	Read	webacl*		
GetPermissionPolicy	Grants permission to retrieve an IAM policy attached to a RuleGroup	Read	rulegroup*		
GetRateBasedRule	Grants permission to retrieve a RateBasedRule	Read	ratebasedrule*		
GetRateBasedRuleManagedKeys	Grants permission to retrieve the array of IP addresses that are currently being blocked by a RateBasedRule	Read	ratebasedrule*		
GetRegexMatchSet	Grants permission to retrieve a RegexMatchSet	Read	regexmatchset*		
GetRegexPatternSet	Grants permission to retrieve a RegexPatternSet	Read	regexpatternset*		
GetRule	Grants permission to retrieve a Rule	Read	rule*		
GetRuleGroup	Grants permission to retrieve a RuleGroup	Read	rulegroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
GetSampledRequests	Grants permission to retrieve detailed information for a sample set of web requests	Read	webacl		
GetSizeConstraintSet	Grants permission to retrieve a SizeConstraintSet	Read	sizeconstraintset*		
GetSqlInjectionMatchSet	Grants permission to retrieve an SqlInjectionMatchSet	Read	sqlinjectionmatchset*		
GetWebACL	Grants permission to retrieve a WebACL	Read	webacl*		
GetWebACLForResource	Grants permission to retrieve a WebACL that's associated with a specified resource	Read	loadbalancer/app/*_*		
GetXssMatchSet	Grants permission to retrieve an XssMatchSet	Read	xssmatchset*		
ListActivatedRulesInRuleGroup	Grants permission to retrieve an array of ActivatedRule objects	List			
ListByteMatchSets	Grants permission to retrieve an array of ByteMatchSetSummary objects	List			
ListGeoMatchSets	Grants permission to retrieve an array of GeoMatchSetSummary objects	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListIPSets	Grants permission to retrieve an array of IPSetSummary objects	List			
ListLoggingConfigurations	Grants permission to retrieve an array of LoggingConfiguration objects	List			
ListRateBasedRules	Grants permission to retrieve an array of RuleSummary objects	List			
ListRegexMatchSets	Grants permission to retrieve an array of RegexMatchSetSummary objects	List			
ListRegexPatternSets	Grants permission to retrieve an array of RegexPatternSetSummary objects	List			
ListResourcesForWebACL	Grants permission to retrieve an array of resources associated with a specified WebACL	List	webacl*		
ListRuleGroups	Grants permission to retrieve an array of RuleGroup objects	List			
ListRules	Grants permission to retrieve an array of RuleSummary objects	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ListSizeConstraintSets	Grants permission to retrieve an array of SizeConstraintSetSummary objects	List			
ListSqlInjectionMatchSets	Grants permission to retrieve an array of SqlInjectionMatchSet objects	List			
ListSubscribedRuleGroups	Grants permission to retrieve an array of RuleGroup objects that you are subscribed to	List			
ListTagsForResource	Grants permission to lists the Tags for a resource	Read	ratebasedrule		
			rule		
			rulegroup		
			webacl		
ListWebACLs	Grants permission to retrieve an array of WebACLSummary objects	List			
ListXssMatchSets	Grants permission to retrieve an array of XssMatchSet objects	List			
PutLoggingConfiguration	Grants permission to associates a LoggingConfiguration with a web ACL	Write	webacl*		iam:CreateServiceLinkedRole

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutPermissionPolicy	Grants permission to attach an IAM policy to a specified rule group, to support rule group sharing between accounts	Permissions management	rulegroup*		
TagResource	Grants permission to add a Tag to a resource	Tagging	ratebasedrule		
			rule		
			rulegroup		
			webacl		
				aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	Grants permission to remove a Tag from a resource	Tagging	ratebasedrule		
			rule		
			rulegroup		
			webacl		
				aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateByteMatchSet	Grants permission to insert or delete ByteMatchTuple objects in a ByteMatchSet	Write	bytematchset*		
UpdateGeoMatchSet	Grants permission to insert or delete GeoMatchConstraint objects in a GeoMatchSet	Write	geomatchset*		
UpdateIPSet	Grants permission to insert or delete IPSetDescriptor objects in an IPSet	Write	ipset*		
UpdateRateBasedRule	Grants permission to insert or delete predicate objects in a rate based rule and update the RateLimit in the rule	Write	ratebasedrule*		
UpdateRegexMatchSet	Grants permission to insert or delete RegexMatchTuple objects in a RegexMatchSet	Write	regexmatchset*		
UpdateRegexPatternSet	Grants permission to insert or delete RegexPatternStrings in a RegexPatternSet	Write	regexpatternset*		
UpdateRule	Grants permission to insert or delete predicate objects in a Rule	Write	rule*		
UpdateRuleGroup	Grants permission to insert or delete ActivatedRule objects in a RuleGroup	Write	rulegroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateSizeConstraintSet	Grants permission to insert or delete SizeConstraint objects in a SizeConstraintSet	Write	sizeconstraintset*		
UpdateSqlInjectionMatchSet	Grants permission to insert or delete SqlInjectionMatchTuple objects in an SqlInjectionMatchSet	Write	sqlinjectionmatchset*		
UpdateWebACL	Grants permission to insert or delete ActivatedRule objects in a WebACL	Permissions management	webacl*		
UpdateXssMatchSet	Grants permission to insert or delete XssMatchTuple objects in an XssMatchSet	Write	xssmatchset*		

Resource types defined by Amazon WAF Regional

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
bytematchset	`arn:${Partition}:waf-regional:${Region}:${Account}:bytematchset/${Id}`	

Resource types	ARN	Condition keys
ipset	arn:${Partition}:waf-regional:${Region}:${Account}:ipset/${Id}	
loadbalancer/app/	arn:${Partition}:elasticloadbalancing:${Region}:${Account}:loadbalancer/app/${LoadBalancerName}/${LoadBalancerId}	
ratebasedrule	arn:${Partition}:waf-regional:${Region}:${Account}:ratebasedrule/${Id}	aws:ResourceTag/${TagKey}
rule	arn:${Partition}:waf-regional:${Region}:${Account}:rule/${Id}	aws:ResourceTag/${TagKey}
sizeconstraintset	arn:${Partition}:waf-regional:${Region}:${Account}:sizeconstraintset/${Id}	
sqlinjectionmatchset	arn:${Partition}:waf-regional:${Region}:${Account}:sqlinjectionset/${Id}	
webacl	arn:${Partition}:waf-regional:${Region}:${Account}:webacl/${Id}	aws:ResourceTag/${TagKey}
xssmatchset	arn:${Partition}:waf-regional:${Region}:${Account}:xssmatchset/${Id}	
regexmatchset	arn:${Partition}:waf-regional:${Region}:${Account}:regexmatch/${Id}	
regexpatternset	arn:${Partition}:waf-regional:${Region}:${Account}:regexpatternset/${Id}	
geomatchset	arn:${Partition}:waf-regional:${Region}:${Account}:geomatchset/${Id}	

Resource types	ARN	Condition keys
rulegroup	`arn:${Partition}:waf-regional:${Region}:${Account}:rulegroup/${Id}`	aws:ResourceTag/${TagKey}

Condition keys for Amazon WAF Regional

Amazon WAF Regional 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 Amazon 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 assoicated with the resource	String
aws:TagKeys	Filters actions based on the presence of mandatory tags in the request	ArrayOfString

Actions, resources, and condition keys for Amazon WAF V2

Amazon 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 Amazon WAF V2
- Resource types defined by Amazon WAF V2
- Condition keys for Amazon WAF V2

Actions defined by Amazon 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 Amazon. 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.

> **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 appsync:SetWebACL cognito-idp:AssociateWebACL ec2:AssociateVerifiedAccess

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
					InstanceWebAcl elasticloadbalancing:SetWebAcl wafv2:GetPermissionPolicy wafv2:PutPermissionPolicy
			amplify-app		
			apigateway		
			apprunner		
			appsync		
			loadbalancer/app/		
			userpool		
			verified-access-instance		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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/${TagKey} aws:TagKeys	
CreateRegexPatternSet	Grants permission to create a RegexPatternSet	Write	regexpatternset*		wafv2:TagResource
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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		
			regexpatternset		
			rulegroup		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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*		
DeleteRegexPatternSet	Grants permission to delete a RegexPatternSet	Write	regexpatternset*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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 Amazon 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 Amazon 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 Amazon 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 Amazon WAF V2

Amazon 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 Amazon 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 Amazon WorkSpaces

Amazon WorkSpaces (service prefix: `workspaces`) 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 WorkSpaces
- Resource types defined by Amazon WorkSpaces
- Condition keys for Amazon WorkSpaces

Actions defined by Amazon WorkSpaces

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 Amazon. 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.

> **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
AcceptAccountLinkInvitation	Grants permission to accept invitations from other Amazon accounts to share the same configuration for WorkSpaces BYOL	Write			
AssociateConnectionAlias	Grants permission to associate connection aliases with directories	Write	connectionalias*		
			directoryid*		
AssociateIpGroups	Grants permission to associate IP access control groups with directories	Write	directoryid*		
			workspaceipgroup*		
AssociateWorkspaceApplication	Grants permission to associate a workspace application with a WorkSpace	Write	workspaceapplication*		
			workspaceid*		
				aws:ResourceTag/	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				${TagKey}	
AuthorizeIpRules	Grants permission to add rules to IP access control groups	Write	workspaceipgroup*		workspaces:UpdateRulesOfIpGroup
CopyWorkspaceImage	Grants permission to copy a WorkSpace image	Write	workspaceimage*		workspaces:DescribeWorkspaceImages
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateAccountLinkInvitation	Grants permission to invite other Amazon accounts to share the same configuration for WorkSpaces BYOL	Write			
CreateConnectClientAddIn	Grants permission to create an Amazon Connect client add-in within a directory	Write	directoryid*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateConnectionAlias	Grants permission to create connection aliases for use with cross-Region redirection	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateIpGroup	Grants permission to create IP access control groups	Write		aws:RequestTag/${TagKey} aws:TagKeys	
CreateStandbyWorkspaces	Grants permission to create one or more Standby WorkSpaces	Write	directoryid*		
			workspaceid*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateTags	Grants permission to create tags for WorkSpaces resources	Tagging		aws:RequestTag/${TagKey} aws:TagKeys	
CreateUpdatedWorkspaceImage	Grants permission to create an updated WorkSpace image	Write	workspaceimage*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkspaceBundle	Grants permission to create a WorkSpace bundle	Write	workspacebundle*		workspaces:CreateTags
			workspaceimage*		
				aws:RequestTag/${TagKey} aws:TagKeys	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
CreateWorkspaceImage	Grants permission to create a new WorkSpace image	Write	workspaceid*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkspaces	Grants permission to create one or more WorkSpaces	Write	directoryid*		
			workspacebundle*		
			workspaceid*		
				aws:RequestTag/${TagKey} aws:TagKeys	
CreateWorkspacesPool	Grants permission to create a WorkSpaces Pool	Write	directoryid*		
			workspacebundle*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
			workspace spoolid*		
				aws:RequestTag/${TagKey} aws:TagKeys	
DeleteAccountLinkInvitation	Grants permission to delete invitations to other Amazon accounts to share the same configuration for WorkSpaces BYOL	Write			
DeleteClientBranding	Grants permission to delete Amazon WorkSpaces Client branding data within a directory	Write	directory id*		
DeleteConnectClientAddIn	Grants permission to delete an Amazon Connect client add-in that is configured within a directory	Write	directory id*		
DeleteConnectionAlias	Grants permission to delete connection aliases	Write	connectionalias*		
DeleteIpGroup	Grants permission to delete IP access control groups	Write	workspace ipgroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DeleteTags	Grants permission to delete tags from WorkSpaces resources	Tagging		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteWorkspaceBundle	Grants permission to delete WorkSpace bundles	Write	workspacebundle*		
DeleteWorkspaceImage	Grants permission to delete WorkSpace images	Write	workspaceimage*		
DeployWorkspaceApplications	Grants permission to deploy all pending workspace applications on a WorkSpace	Write	workspaceid*		
				aws:ResourceTag/${TagKey}	
DeregisterWorkspaceDirectory	Grants permission to deregister directories from use with Amazon WorkSpaces	Write	directoryid*		
DescribeAccount	Grants permission to retrieve the configuration of Bring Your Own License (BYOL) for WorkSpaces accounts	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeAccountModifications	Grants permission to retrieve modifications to the configuration of Bring Your Own License (BYOL) for WorkSpaces accounts	Read			
DescribeApplicationAssociations	Grants permission to retrieve information about resources associated with a WorkSpace application	List	workspaceapplication*		
				aws:ResourceTag/${TagKey}	
DescribeApplications	Grants permission to obtain information about WorkSpace applications	List			
DescribeBundleAssociations	Grants permission to retrieve information about resources associated with a WorkSpace bundle	List	workspacebundle*		
				aws:ResourceTag/${TagKey}	
DescribeClientBranding	Grants permission to retrieve Amazon WorkSpaces Client branding data within a directory	Read	directoryid*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeClientProperties	Grants permission to retrieve information about WorkSpaces clients	List	directoryid*		
DescribeConnectClientAddIns	Grants permission to retrieve a list of Amazon Connect client add-ins that have been created	List	directoryid*		
DescribeConnectionAliasPermissions	Grants permission to retrieve the permissions that the owners of connection aliases have granted to other Amazon accounts for connection aliases	Read	connectionalias*		
DescribeConnectionAliases	Grants permission to retrieve a list that describes the connection aliases used for cross-Region redirection	Read			
DescribeImageAssociations	Grants permission to retrieve information about resources associated with a WorkSpace image	List	workspaceimage*		
				aws:ResourceTag/${TagKey}	
DescribeIpGroups	Grants permission to retrieve information about IP access control groups	Read	workspaceipgroup*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeTags	Grants permission to describe the tags for WorkSpaces resources	Read			
DescribeWorkspaceAssociations	Grants permission to retrieve information about resources associated with a WorkSpace	List	workspaceid*		
				aws:ResourceTag/${TagKey}	
DescribeWorkspaceBundles	Grants permission to obtain information about WorkSpace bundles	List			
DescribeWorkspaceDirectories	Grants permission to retrieve information about directories that are registered with WorkSpaces	Read			
DescribeWorkspaceImagePermissions	Grants permission to retrieve information about WorkSpace image permissions	Read	workspaceimage*		
DescribeWorkspaceImages	Grants permission to retrieve information about WorkSpace images	List			
DescribeWorkspaceSnapshots	Grants permission to retrieve information about WorkSpace snapshots	List	workspaceid*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
DescribeWorkspaces	Grants permission to obtain information about WorkSpaces	List			
DescribeWorkspacesConnectionStatus	Grants permission to obtain the connection status of WorkSpaces	Read			
DescribeWorkspacesPoolSessions	Grants permission to retrieve information about the sessions of a WorkSpaces Pool	List	workspacespoolid*		
DescribeWorkspacesPools	Grants permission to retrieve information about WorkSpaces Pools	List			
DisassociateConnectionAlias	Grants permission to disassociate connection aliases from directories	Write	connectionalias*		
DisassociateIpGroups	Grants permission to disassociate IP access control groups from directories	Write	directoryid*		
			workspaceipgroup*		
DisassociateWorkspaceApplication	Grants permission to disassociate a workspace application from a WorkSpace	Write	workspaceapplication*		
			workspaceid*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				aws:ResourceTag/${TagKey}	
GetAccountLink	Grants permission to retrieve a link with another Amazon Account for sharing configuration for WorkSpaces BYOL	Read			
ImportClientBranding	Grants permission to import Amazon WorkSpaces Client branding data within a directory	Write	directoryid*		
ImportWorkspaceImage	Grants permission to import Bring Your Own License (BYOL) images into Amazon WorkSpaces	Write			ec2:DescribeImages ec2:ModifyImageAttribute
ListAccountLinks	Grants permission to retrieve links with the Amazon Account(s) that share your configuration for WorkSpaces BYOL	List			
ListAvailableManagementCidrRanges	Grants permission to list the available CIDR ranges for enabling Bring Your Own License (BYOL) for WorkSpaces accounts	List			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
MigrateWorkspace	Grants permission to migrate WorkSpaces	Write	workspacebundle*		
			workspaceid*		
ModifyAccount	Grants permission to modify the configuration of Bring Your Own License (BYOL) for WorkSpaces accounts	Write			
ModifyCertificateBasedAuthProperties	Grants permission to modify the certificate-based authorization properties of a directory	Write	directoryid*		
ModifyClientProperties	Grants permission to modify the properties of WorkSpaces clients	Write	directoryid*		
ModifyEndpointEncryptionMode	Grants permission to configure the specified directory between Standard TLS and FIPS 140-2 validated mode	Write	directoryid*		
ModifySamlProperties	Grants permission to modify the SAML properties of a directory	Write	directoryid*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
ModifySelfservicePermissions	Grants permission to modify the self-service WorkSpace management capabilities for your users	Permissions management	directoryid*		
ModifyStreamingProperties	Grants permission to modify the streaming properties	Write	directoryid*		
ModifyWorkspaceAccessProperties	Grants permission to specify which devices and operating systems users can use to access their WorkSpaces	Write	directoryid*		
ModifyWorkspaceCreationProperties	Grants permission to modify the default properties used to create WorkSpaces	Write	directoryid*		
ModifyWorkspaceProperties	Grants permission to modify WorkSpace properties, including the running mode and the AutoStop period	Write	workspaceid*		
ModifyWorkspaceState	Grants permission to modify the state of WorkSpaces	Write	workspaceid*		
RebootWorkspaces	Grants permission to reboot WorkSpaces	Write	workspaceid*		
RebuildWorkspaces	Grants permission to rebuild WorkSpaces	Write	workspaceid*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
RegisterWorkspaceDirectory	Grants permission to register directories for use with Amazon WorkSpaces	Write	directoryid*		
				aws:RequestTag/${TagKey} aws:TagKeys	
RejectAccountLinkInvitation	Grants permission to reject invitations from other Amazon accounts to share the same configuration for WorkSpaces BYOL	Write			
RestoreWorkspace	Grants permission to restore WorkSpaces	Write	workspaceid*		
RevokeIpRules	Grants permission to remove rules from IP access control groups	Write	workspaceipgroup*		workspaces:UpdateRulesOfIpGroup
StartWorkspaces	Grants permission to start AutoStop WorkSpaces	Write	workspaceid*		
StartWorkspacesPool	Grants permission to start a WorkSpaces Pool	Write	workspacespoolid*		
StopWorkspaces	Grants permission to stop AutoStop WorkSpaces	Write	workspaceid*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
StopWorkspacesPool	Grants permission to stop a WorkSpaces Pool	Write	workspacespoolid*		
Stream	Grants permission to federated users to sign in by using their existing credentials and stream their workspace	Write	directoryid*		
				workspaces:userId	
TerminateWorkspaces	Grants permission to terminate WorkSpaces	Write	workspaceid*		
TerminateWorkspacesPool	Grants permission to terminate a WorkSpaces Pool	Write	workspacespoolid*		
TerminateWorkspacesPoolSession	Grants permission to terminate a WorkSpaces Pool session	Write			
UpdateConnectClientAddIn	Grants permission to update an Amazon Connect client add-in. Use this action to update the name and endpoint URL of an Amazon Connect client add-in	Write	directoryid*		
UpdateConnectionAliasPermission	Grants permission to share or unshare connection aliases with other accounts	Permissions management	connectionalias*		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
UpdateRulesOfIpGroup	Grants permission to replace rules for IP access control groups	Write	workspaceipgroup*		workspaces:AuthorizeIpRules workspaces:RevokeIpRules
UpdateWorkspaceBundle	Grants permission to update the WorkSpace images used in WorkSpace bundles	Write	workspacebundle*		
			workspaceimage*		
UpdateWorkspaceImagePermission	Grants permission to share or unshare WorkSpace images with other accounts by specifying whether other accounts have permission to copy the image	Permissions management	workspaceimage*		
UpdateWorkspacesPool	Grants permission to update the WorkSpaces pool	Write	workspacespoolid*		

Resource types defined by Amazon WorkSpaces

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
directoryid	arn:${Partition}:workspaces:${Region}:${Account}:directory/${DirectoryId}	aws:ResourceTag/${TagKey}
workspacebundle	arn:${Partition}:workspaces:${Region}:${Account}:workspacebundle/${BundleId}	aws:ResourceTag/${TagKey}
workspaceid	arn:${Partition}:workspaces:${Region}:${Account}:workspace/${WorkspaceId}	aws:ResourceTag/${TagKey}
workspaceimage	arn:${Partition}:workspaces:${Region}:${Account}:workspaceimage/${ImageId}	aws:ResourceTag/${TagKey}
workspaceipgroup	arn:${Partition}:workspaces:${Region}:${Account}:workspaceipgroup/${GroupId}	aws:ResourceTag/${TagKey}
workspacespoolid	arn:${Partition}:workspaces:${Region}:${Account}:workspacespool/${PoolId}	aws:ResourceTag/${TagKey}
connectionalias	arn:${Partition}:workspaces:${Region}:${Account}:connectionalias/${ConnectionAliasId}	aws:ResourceTag/${TagKey}
workspaceapplication	arn:${Partition}:workspaces:${Region}:${Account}:workspaceapplication/${WorkSpaceApplicationId}	aws:ResourceTag/${TagKey}

Condition keys for Amazon WorkSpaces

Amazon WorkSpaces 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 Amazon 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
workspaces:userId	Filters access by the ID of the Workspaces user	String

Actions, resources, and condition keys for Amazon X-Ray

Amazon 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 Amazon X-Ray

- Resource types defined by Amazon X-Ray
- Condition keys for Amazon X-Ray

Actions defined by Amazon 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 Amazon. 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.

> **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			
CreateGroup	Grants permission to create a group resource with a name and a filter expression	Write	group*		
				aws:RequestTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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			
DeleteSamplingRule	Grants permission to delete a sampling rule	Write	sampling-rule*		
				aws:ResourceTag/${TagKey}	

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
GetInsight	Grants permission to retrieve the details of a specific insight	Read			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
GetSamplingTargets	Grants permission to request a sampling quota for rules that the service is using to sample requests	Read			

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

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
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			
PutSpans	Grants permission to upload OpenTelemetry spans to Amazon X-Ray	Write			
PutSpansForIndexing [permission only]	Grants permission to upload spans to Amazon X-Ray to be indexed	Write			
PutTelemetryRecords	Grants permission to send Amazon X-Ray daemon telemetry to the service	Write			

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
PutTraceSegments	Grants permission to upload segment documents to Amazon X-Ray. The X-Ray SDK generates segment documents and sends them to the X-Ray daemon, which uploads them in batches	Write			
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		
				aws:TagKeys aws:RequestTag/${TagKey}	
UntagResource	Grants permission to remove tags from an X-Ray resource	Tagging	group		
			sampling-rule		

Actions	Description	Access level	Resource types (*required)	Condition keys	Dependent actions
				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}	
UpdateTraceSegmentDestination	Grants permission to modify the destination of data sent to PutTraceSegments and OpenTelemetry API	Write			

Resource types defined by Amazon 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 Amazon X-Ray

Amazon 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 Amazon 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

Related resources

For related information found in the *IAM User Guide*, see the following resources:

- Tutorial: Create and attach your first customer managed policy
- Amazon services that work with IAM
- Policy evaluation logic

Simplified Amazon Web Services service information for programmatic access

Amazon provides service reference information in JSON format to streamline the automation of policy management workflows. With the service reference information, you can access available actions, resources, and condition keys across Amazon Web Services services from machine-readable files. Security administrators can establish guardrails and developers can ensure appropriate access to applications by identifying the available actions, resources, and condition keys for each Amazon Web Services service. Amazon provides service reference information for Amazon Web Services 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 Amazon Web Services service.

Actions, resources, and condition keys for services that share a service prefix may be split across multiple pages in the Service Authorization Reference.

> **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 Amazon Web Services service reference information

1. Navigate to the service reference information to access the list of Amazon Web Services 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"
    },
    …
]
```

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"
            ],
            "Resources": [
                {
                    "Name": "object"
                }
            ]
        },
        {
            "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"
            ],
            "Resources": [
                {
                    "Name": "bucket"
                }
            ]
        },
        ...
    ],
    "ConditionKeys": [
        {
            "Name": "s3:TlsVersion",
            "Types": [
                "Numeric"
            ]
        },
        {
            "Name": "s3:authType",
            "Types": [
                "String"
            ]
        },
        ...
    ],
    "Resources": [
        {
            "Name": "accesspoint",
            "ARNFormats": [
                "arn:${Partition}:s3:${Region}:${Account}:accesspoint/
${AccessPointName}"
            ]
        },
        {
            "Name": "bucket",
```

```
            "ARNFormats": [
                "arn:${Partition}:s3:::${BucketName}"
            ]
        }
        ...
    ],
    "Version": "v1.1"
}
```

3. Download the JSON file from the service URL to use in your policy authoring workflows.